Department for Science, Innovation and Technology – Written Evidence (DAT0013)

HM Government - Department of Science, Innovation and Technology – Written Evidence

House of Lords EU Affairs Committee inquiry:

UK-EU data adequacy

Executive summary

1. **Maintaining data adequacy between the UK and the EU facilitates the free flow of personal data,** keeping compliance costs low for businesses and the public safe in both jurisdictions. The two adequacy decisions that the EU granted to the UK in 2021 - for the general processing of personal data under the EU GDPR and the processing of personal data for law enforcement purposes under the Law Enforcement Directive are to be reviewed by the EU by 27 June 2025.
2. **HM Government believes that the UK's reforms are compatible with maintaining adequacy decisions from the EU.** The UK has a near-identical regime to the EU GDPR, which it is now reforming through the Data Protection and Digital Information (DPDI) Bill. Many of the key elements, such as the data protection principles, remain unchanged in recognition of the fact that they provide a high level of protection for people's personal data.
3. **In the unlikely event of a no-adequacy scenario, personal data can still flow from the EU to the UK**, as organisations can rely on alternative transfer mechanisms. However, this would add compliance costs and reduce the level of trade. For law enforcement data processing, maintaining EU adequacy decisions is not a legal prerequisite for cooperation under Part 3 of the UK-EU Trade and Cooperation Agreement.
4. **The UK is committed to championing international data flows while maintaining the high standards of data protection** provided by UK law. Any future transfer mechanism such as a new data bridge decision or recognised tool must meet our robust data protection standards.

1. **What is your assessment of the existing adequacy arrangement underpinning data flows between the UK and the European Union?**

5. The EU and UK respective arrangements for the free flow of personal data allow organisations to transfer data in an easy and safe way. Maintaining the free flow of personal data with the EU, the UK's largest trading partner, is important. In 2022 alone, the overall value of UK-EU trade amounted to £772 billion, with £161 billion estimated to be data-enabled trade.

6. In 2021, following the UK's exit from the EU, the European Commission assessed the UK's data protection framework and granted the UK two adequacy decisions. The first applies to any organisation subject to the EU GDPR and the second to data processing for law enforcement purposes subject to the Law Enforcement Directive. These decisions are required to be reviewed and renewed by the EU by 27 June 2025. The UK, at the same time, also independently legislated to allow the free flow of personal data to EEA states and EU institutions under the UK GDPR and EEA states under Part 3 of the Data Protection Act (DPA) 2018.

7. These arrangements ensured that there was no disruption to the free flow of personal data, providing certainty to UK and EU organisations. The free flow of personal data keeps organisations' compliance costs low, removes barriers to trade and innovation and helps to keep the public safe in both the UK and the EU. Without these arrangements, individual organisations would have to implement potentially costly or time intensive alternative transfer mechanisms - for example, using one of the available appropriate safeguards, such as a legally binding instrument or a contract incorporating standard data protection clauses.

8. The upcoming adequacy review of the UK by the EU is an opportunity to maintain and grow the volume of data flowing into the UK and ensure the continuity of the UK's adequate status in the long term.

9. The requirement to review and renew the EU's adequacy decisions for the UK by 2025 was also reflective of the UK's ambitions to reform its data protection laws to remove burdens for businesses whilst maintaining the UK's high data protection standards. The Data Protection and Digital Information (DPDI) Bill makes targeted amendments to the UK GDPR and Data Protection Act 2018 whilst other relevant pieces of legislation, such as the Investigatory Powers

(Amendment) Act 2024, updated targeted elements of the Investigatory Powers Act 2016.

a. What is your assessment of the value of the EU's adequacy decisions to UK organisations?

10. Data flows enable significant levels of bilateral trade and support the growth of our digital economy. UK organisations of all sizes and across all sectors rely on various services from overseas, such as email marketing, online retail, communication platforms and cloud storage. In 2022 alone, the overall value of UK-EU trade amounted to £772 billion, with £161 billion estimated to be data-enabled trade[1].

11. Data flows are not just about enabling international commerce and trade – they are also about facilitating greater innovation, research and development and keeping citizens safe through effective cooperation on law enforcement. A key example is the coronavirus pandemic, where we needed to share data quickly and responsibly to develop treatment methods for the public good.

12. If our adequacy decisions were not renewed, this would have a significant impact across the EU and the UK. Indeed, in that scenario, EU organisations would have to implement alternative transfer mechanisms to send data to the UK, raising legal and compliance obligations for both EU and UK organisations.

13. For the UK, the estimated economic impact of maintaining EU adequacy is between £190 and £460 million in compliance costs savings for UK businesses and an annual benefit of between £210 and £420 million in retained export revenue. Once appraised over a 10-year period, the estimated Net Present Value (2019 prices, 2020 present value) of EU adequacy being continued is £2 billion (range of £1.6 and £3.4 billion)[2].

14. The European Union and its Member States equally continue to be important partners to UK law enforcement agencies to tackle crime and bring offenders to justice and the free flow of personal data enabled by law enforcement adequacy is at the heart of cross border cooperation. EU adequacy decisions for the UK, and similar UK arrangements for the

[1] DSIT internal analysis on the world total of UK services exports, based on 2022 ONS published statistics, in sectors defined as data-enabled by UNCTAD (United Nations Conference on Trade and Development).
[2] Data Protection and Digital Information Bill (No.2) Impact Assessment, DSIT (2023)

EU, help to minimise cost and burdens for law enforcement agencies on both sides exchanging data to support these activities.

b. How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?

15. The GDPR came into force across the EU in May 2018. Part 2 of the Data Protection Act 2018 implemented aspects of the GDPR where Member States had the flexibility to derogate and/or provide exemptions in relation to specific GDPR provisions. The Law Enforcement Directive was transposed into UK law at the same time through Part 3 of the Data Protection Act 2018. Since then, the UK has left the EU. Between September and November 2021, HM Government consulted on possible improvements to the legislation with a view to reducing unnecessary compliance burdens on organisations; making aspects of the law clearer and simpler to promote innovation and research; and improving the operational effectiveness of the law enforcement agencies, whilst maintaining high standards of data protection.

16. The Data Protection and Digital Information Bill, currently before the UK Parliament, delivers some of these changes. The proposals in the Bill, for example the requirement to keep records only in relation to high-risk processing activities, are estimated to achieve annual compliance cost savings of £129.3 million for businesses; details of projected savings can be viewed in HM Government's impact assessment – see in particular, paragraphs 518 and 519. However, it is important to note that many of the key elements of the legislation, such as the data protection principles, remain unchanged in recognition of the fact that they provide a high level of protection for people's personal data.

17. Likewise, the existing framework under Parts 3 and 4 of the DPA for law enforcement and intelligence service processing works well overall, but as Parliament and the public would expect, we keep our framework under review and will amend if parts do not operate as they should. For example, the 2021 consultation '*Data: a new direction'* highlighted the need to provide greater consistency across processing regimes and to make the rules clearer to support operational partners in adopting new technologies to protect the public.

18. HM Government cannot comment on the functioning of the Law Enforcement Directive itself, but notes that the European Commission published its own report on its functioning in 2022 which concluded that the LED was overall an effective tool for law enforcement cooperation within the EU.

c. How would you assess the overall performance and effectiveness of the Information Commissioner's Office (ICO) as the UK's independent data regulator? Has its work been impacted by decisions on data adequacy?

19. The ICO is recognised as a world leading data protection regulator. It has a strong track record of upholding information rights and privacy, as well as providing guidance and support for organisations who are using personal data. Moreover, the ICO plays a crucial role in upholding and developing information rights practices internationally.

20. The Information Commissioner is directly accountable to Parliament through the Parliamentary Select Committees, before which the Commissioner usually appears two to four times per year. Some of the (non-exhaustive) examples of its recent actions that demonstrate its activities include:

- Taken regulatory actions against Snap relating to a potential failure to properly assess the privacy risks posed by its generative AI chatbot 'My AI';
- Signed onto a new international multilateral agreement with the Global Cooperation Arrangement for Privacy Enforcement to cooperate in cross-border data protection and privacy enforcement;
- Published guidance to improve transparency in health and social care.

21. Between September and November 2021, HM Government consulted on potential reforms to the ICO as part of as part of broader efforts to reshape the UK's approach to data protection. The ICO has a strong track record of upholding information rights and privacy, but the digital landscape is rapidly evolving, and our regulatory approach must evolve with it, whilst maintaining high standards of data protection.

22. The DPDI Bill will strengthen and modernise the ICO by ensuring it has the capabilities and powers to tackle organisations who breach data rules, empowering it to better allocate its resources, and providing it with a new strategic framework that will provide certainty

and clarity to the Commissioner, to underpin and empower its regulation of the UK's data protection regime. The new framework also introduces several new duties that the ICO should consider when exercising its functions, to reflect the ICO's important cross-economy role. These will strengthen the ICO's existing obligations, ensuring it is empowered and equipped to factor in interactions with other areas.

23. DSIT has worked and will continue to work closely with the ICO on new data bridges as they develop, including consulting with the ICO as required by the legislation.

2. What are the possible challenges to UK-EU data adequacy regime?

24. The UK has entered a new phase in its relationship with the EU, following EU exit. The 2023 Integrated Review refresh highlights the importance of reinvigorating the UK's European relationships and notes: *"our ambition is to build even stronger relationships with our European allies and partners based on values, reciprocity and cooperation across our shared interests. This includes the EU, with which we seek to work closely in areas of mutual benefit*".

25. In the field of data protection, the UK and EU are like-minded partners that share a strong commitment to upholding and promoting high data protection standards. Our respective arrangements for the free flow of personal data reflect this shared commitment and have enabled closer cooperation with the EU on data flows issues, for example via the EU's High-level Roundtable on Safe Data flows, an event bringing together EU adequate countries, that the DSIT Minister for Data and the UK Information Commissioner attended in March 2024. The UK is working with the European Commission and EU Member States in multilateral fora to find solutions to the global challenges around privacy and security. This includes building on existing achievements in the form of promoting the OECD Principles on Privacy and Trusted Government Access to Data Held in the Private Sector alongside leveraging the Data Free Flow with Trust agenda at the G7 and via the OECD's Expert Community to overcome shared challenges.

26. UK Ministers recognise the importance of adequacy and are committed to continue building on our positive, constructive relationship with the EU. Since 2021, when the consultation "Data: A New Direction" was published, HM Government has held a number of technical discussions with the European Commission to ensure the rationale and safeguards

of our reforms are understood. Adequacy does not require the UK to mirror exactly the EU's GDPR approach and we note that other adequate third countries have started from very different data protection legal frameworks. HM Government remains committed to working closely with the EU as the DPDI Bill progresses through Parliament and to engage regularly with European counterparts, including the European Commission, to ensure the successful conclusion of its review. HM Government can see no reason why the proposed reforms should not be compatible with renewing our EU adequacy decisions.

27. The EU's adequacy decision for the UK currently excludes transfers of data processed for immigration purposes, which was based on issues that have now been resolved through secondary legislation. During its review, we expect the EU may evaluate the enhanced rules and whether the exclusion of immigration data remains necessary.

a. What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

28. The EU's published methodology for granting countries data adequacy can be found in its Report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC. The EU's test for adequacy requires that a country or international organisation provides an 'essentially equivalent' level of protection to the EU. The Court of Justice of the European Union (CJEU) has been clear that 'essential equivalence' does not require point-by-point replication of the EU GDPR and recognised that countries with different privacy systems and legal traditions can meet this standard.

29. The criteria for the European Commission's assessment of the UK are set out in Article 45 of EU GDPR and Article 36 of the Law Enforcement Directive. Under Article 45 of EU GDPR, the European Commission will consider the UK's data protection regime; rule of law; respect for human rights and fundamental freedoms; existence and effective functioning of independent supervisory authorities; international commitments; and rules governing government access to data for law enforcement and national security purposes. Additional factors for consideration will also be drawn from relevant CJEU case law, such as *Schrems I* and *II*, as well as the European Data Protection Board (EDPB) adequacy referential.

30. However, for the upcoming review of the UK, the European Commission may examine what has changed since the last adequacy decision in 2021, rather than starting from scratch. In their recent review of the eleven countries with existing adequacy arrangements, the European Commission considered new legislation

and international commitments and they may take a similar approach with the UK.

b. What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

31. Individuals, civil society organisations and Members of the European Parliament have the right to challenge any EU adequacy decisions at the CJEU, although a challenge has not been brought on the EU's adequacy decisions for the UK since they were adopted in 2021.

32. In the case of a UK-EU adequacy challenge, the CJEU could potentially be asked to interpret the law for a national court and/or annul the relevant adequacy decision itself if it was believed to violate EU treaties or fundamental rights. In practice, the CJEU would likely determine whether the European Commission has been right in its assessment that the UK provides an 'essentially equivalent' standard of data protection based on EU GDPR's Article 45 criteria.

33. It is difficult to predict the precise factors that could be considered in relation to the legality of the EU's adequacy decisions for the UK and would be specific to the case being brought and the route by which it was challenged.

c. How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?

34. Automated Decision Making (ADM) is increasingly AI-driven and, with the expansion in use of this technology, it is important that our rules are fit for purpose. HM Government's reforms will help reduce the barriers to responsible data use, and ensure important safeguards are implemented when they matter most. We are expanding the legal bases on which solely ADM can be carried out under the data protection regime, reflecting the growth in use of this processing by emerging technology in everyday life.

35. HM Government reforms will mean that data subjects will have a right to specific safeguards where solely ADM has significant effects on them, regardless of the lawful basis on which this processing is undertaken. These safeguards include providing the data subject with information about the decisions taken about them, and the right to contest those decisions. Controllers will be required to respect data subjects' rights and enable them to make representations about the decisions and obtain human intervention in relation to such decisions.

36. The ADM reforms include a prohibition on use of special category data for ADM purposes except under specific conditions. Under the reforms, where an

organisation processes special category data for ADM on the basis of either contract or the processing being authorised by law, it also has to demonstrate that such processing is necessary for substantial public interest. The only other condition for processing special category data for ADM is through explicit consent. This maintains the protections for special category/sensitive data in relation to ADM as set out in the EU GDPR and Part 3 of the Data Protection Act. The existing transparency and rights of access provisions in the wider data protection framework, which require organisations to inform individuals about the existence of solely ADM, continue to apply to the reformed Article 22. The overarching principle of fairness applies to all ADM processing and, combined with the transparency principles and specific rights in the UK GDPR and Data Protection Act and the safeguards set out in the reformed Article 22 and sections 49 and 50, would require controllers to take suitable measures to review, at the data subject's request, and correct decisions if they have produced an unfair outcome.

37. In addition to the continuing levels of protection for special category data subject to ADM, the existing transparency and rights of access provisions in the wider data protection framework, which require organisations to inform individuals about the existence of solely ADM, continue to apply to the reformed Article 22. The overarching principle of fairness applies to all ADM processing and, combined with the transparency principles and specific rights in the UK GDPR and the safeguards set out in the reformed Article 22, would require controllers to take suitable measures to review, at the data subject's request, and correct decisions if they have produced an unfair outcome.

38. It is DSIT's view that these reforms maintain a high standard of data protection for data subjects and are compatible with maintaining EU adequacy.

39. The AI and machine learning reforms in the Data Protection and Digital Information Bill, including ADM reforms, are estimated to save businesses £2.6 million in compliance cost savings annually. The reforms are also expected to encourage the responsible use of data in AI and machine learning and increase productivity, leading to an estimated £5.6 million annual increase in Gross Value Added (GVA)[3].

3. What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?

40. The absence of EU data adequacy decisions for the UK does not mean that personal data cannot flow from the EU. In that scenario, EU organisations would still be able to rely on alternative transfer mechanisms set out in the EU GDPR or Law Enforcement Directive to transfer personal data to the UK (e.g., Standard Contractual Clauses (SCCs), Binding Corporate Rules).

[3] Data Protection and Digital Information Bill (No.2) Impact Assessment, DSIT (2023)

41. The UK has made its own unilateral data bridge arrangements for the transfer of personal data to the EU which means that, in a context of disruption, the free flow of personal data from the UK to the EU would not be automatically suspended.

42. If the EU revoked its adequacy decision under the Law Enforcement Directive, it would be more difficult to cooperate with the EU to prevent crime and bring perpetrators to justice. Law enforcement authorities in the EU would be required to use alternative transfer mechanisms to transfer data to UK law enforcement authorities.

43. For further details on the range of alternative transfer mechanisms available in a no-adequacy scenario, please see Annex A.

a. Do you have any concerns about the direction of travel of the UK Government's data policies as set out in the Data Protection and Digital Information Bill, and about the potential for greater divergence from EU data standards?

44. The UK is firmly committed to maintaining high data protection standards - now and in the future. We will continue to operate a high-quality regime that promotes growth and innovation, and underpins the trustworthy use of data.

45. While the DPDI Bill will remove the more prescriptive elements of the GDPR, the UK will maintain its high standards of data protection and continue to have one of the closest regimes to the EU in the world.

46. As the European Commission itself has made clear, a third country is not required to have exactly the same rules as the EU to be considered adequate. Indeed, there are fourteen other countries which have EU adequacy, including Japan, the Republic of Korea and Canada. All of these nations pursue independent and often more divergent approaches to data protection. Some EU adequate countries have taken a different approach to the GDPR but have still succeeded in maintaining high data protection standards and securing an adequacy decision from the EU.

47. HM Government maintains an ongoing dialogue with the EU and has a positive, constructive relationship and will continue to engage with the EU, both at official and Ministerial levels, with a view to ensuring our data adequacy decisions can remain in place.

b. How high is the risk of the European Commission withdrawing its UK data adequacy decisions? What impact would that have and how prepared are businesses or the public sector for such a scenario?

48. Given that the UK's data protection framework maintains high standards, HM Government can see no reason why the adequacy decisions could not be retained. Whilst adequacy assessments are for the EU to decide, HM

Government is confident that legislative reforms have been designed with robust safeguards and protections at their core.

49. The withdrawal of adequacy for the UK could have a significant impact to adequacy as a transfer mechanism in the EU context. Indeed, after implementation of the UK's proposed legislative reforms, the UK would continue to have one of the closest data protection regimes to the EU in the world. To date, the European Commission has not revoked or suspended an adequacy decision, although the CJEU has struck down two adequacy decisions.

50. DSIT is keeping other relevant government departments and Devolved Administrations updated on discussions with the European Commission and will increase the frequency when the review begins.

c. What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?

51. Adequacy is not a legal prerequisite for cooperation under Part 3 of the UK-EU Trade & Cooperation Agreement (TCA). Alternative transfer mechanisms as foreseen in the Law Enforcement Directive are available to organisations that wish to transfer data from the EU in a no-adequacy scenario.

52. In this regard, it is notable that Part 3 of the TCA includes a commitment from both sides to a series of shared data protection principles drawn from wider international commitments, including the Council of Europe's Convention 108 on data protection.

53. The adequacy process and decision is a separate process from the TCA. However, both sides have the ability to suspend Part 3 of the TCA if there are "serious and systemic deficiencies" in the respective data protection frameworks, including where such deficiencies lead to the loss of an adequacy decision. This is, however, not automatic.

54. HM Government is confident that our wider reforms are consistent with our broader goal to maintain high standards of data protection and therefore are compatible to maintaining adequacy and pose no risk to the continued operation of the TCA.

4. What can be learned from other countries' experience with the adequacy system and engagement with the European Commission's process?

55. HM Government cannot comment on other jurisdiction's experiences of the EU adequacy system. However, the European Commission has set out the process for how they assess jurisdictions. This process involves a two-way engagement between the EU and the assessed country in Report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC. This engagement can include the exchange of written

materials for the EU to assess. Regular dialogue is an important feature of this process.

56. Following our own experience of obtaining EU adequacy in 2021, the EU adequacy assessment process has demonstrated the importance of having an open and trusted dialogue between like-minded partners. The UK maintains a positive, constructive relationship with the EU and is committed to continue building on this relationship as we approach the review of our adequacy decisions.

a. What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?

57. The European Commission's review of the adequate countries highlighted that although a number of countries continue to have data protection frameworks that take a different approach in protecting personal data from GDPR, they have still been deemed to meet the high standards of the EU adequacy test.

58. HM Government welcomes the EU's reviews on the 11 pre-GDPR adequacy decisions as it evidences the high standards of data protection being upheld in the adequate third countries.

b. Are there examples of best practice which the UK could learn from in the way other countries approach their data transfer arrangements with the EU?

59. The UK maintains high data protection standards when transferring personal data internationally and maintains an open and transparent dialogue with the EU on data transfers. Third countries in receipt of EU adequacy decisions maintain many different approaches to data protection and data transfers that are reflective of their own cultural and historical background.

60. In August 2021, under the "UK approach to international data transfers" mission statement, the UK committed to championing international flows of data under the National Data Strategy. This included a stated aim to work globally to strike data bridge agreements with our partners, deliver innovative alternative mechanisms and remove unjustified barriers to international data transfers. The UK maintains a flexible, outcomes-focused approach to establishing data bridges that could support the UK's ambition to take a more internationally scalable approach to data transfers.

c. What are the implications for the UK's EU adequacy status if the UK grants its own adequacy decisions to other third countries currently not subject to EU adequacy?

61. The UK maintains high data protection standards when transferring personal data internationally. As stated in the August 2021 mission statement “International data transfers: building trust, delivering growth and firing up innovation”, it is the UK’s ambition to independently strike new data bridges with international partners which, following a rigorous assessment, are found to have high data protection standards. The UK’s robust and detailed assessments for a bridge considers the overall effect of a third country’s data protection laws, implementation, enforcement, and supervision.

62. The reforms to the international transfers regime under the DPDI Bill clarify the UK’s framework that regulates the free flow of personal data between the UK and other countries. They tackle the uncertainty and instability in the current data protection framework - not least due to the competing and fragmented interpretations of the same regime. They will allow the UK to continue to be pragmatic in its approach to assessing third countries, reflecting what is right for UK interests.

63. The UK’s proposed changes within the Bill to the international transfers regime do not undermine the substance of the existing adequacy test. The reforms will build upon the existing high standards the UK has for assessing the adequacy of third countries and continue to take into account human rights, rule of law and the existence of an effective data protection regulator. Ultimately, the DSIT Secretary of State must be satisfied that the standard of protection in the other country is not materially lower than the standard of protection in the UK. DSIT has assessed that the UK’s proposed reforms to the international transfers regime will remain compatible with maintaining EU adequacy.

64. On law enforcement, the only jurisdictions that have received an adequacy decision from the UK that are not also considered adequate for law enforcement transfers by the European Commission are the Bailiwicks of Guernsey and Jersey. They respectively received their law enforcement adequacy regulations from the UK in July 2023 and November 2023 following a robust assessment. Following these regulations made by the UK, no concerns were raised by the European Commission.

d. If the UK joined the Global Cross Border Privacy Rules system, what impact if any could that have on the UK’s EU adequacy status?

65. Membership of the Global Cross Border Privacy Rules (CBPR) Forum is compatible with EU adequacy. The Republic of Korea, Japan and Canada are members of the Forum and have positive adequacy decisions from the EU.

66. The UK is committed to championing international data flows while maintaining the high standards of data protection provided by UK law and any new transfer tool must meet the UK’s data protection standards under Article 46 UK GDPR.

67. The UK wants to use our international data transfers framework in a creative and pragmatic way to facilitate data flows on a global scale, as international data flows are becoming increasingly complex.

68. We want to work closely with our international partners to build consensus and shape practical, real-world solutions, of which the Global CBPR (Cross-Border Privacy Rules) System is an example. Indeed, the CBPR system, including the PRP (Privacy Recognition for Processors) system, is one of the very few existing and operational multilateral frameworks that promotes interoperability with multiple jurisdictions. The UK was the first country to secure 'Associate' status in the Global CBPR Forum ('the Forum') in 2023. We are committed to engaging in discussions with the Forum and its like-minded partners to shape the future of the Global CBPR and PRP (Privacy Recognition for Processors) Systems.

69. **Annex A: Question 3 - Alternative transfer mechanisms available in a no adequacy scenario.**

<u>EU GDPR</u>

1. **EU Standard Contractual Clauses** (known as the International Data Transfer Agreements in the UK) **and bespoke contractual clauses** - this is the most used transfer mechanism, which includes a set of legally binding obligations on how data should be processed;

2. **Binding Corporate Rules** - these facilitate data transfers among companies in the same corporate group and considered one of the most robust transfer mechanisms;

3. **Legally binding instruments** between public authorities or bodies –such as a legally binding treaty

4. **Administrative arrangements** between public authorities or bodies – such as a non-legally binding Memorandum of (MoU), approved by the Supervisory Authority.

5. **Approved codes of conduct –** these need to be approved by the regulator and provide companies with binding and enforceable commitments. Different business sectors develop their own codes of conduct that are tailored to their requirements; and

6. **Approved certification schemes** - these demonstrate a company's compliance with the GDPR.

In the absence of an adequacy decision, or of Alternative Transfer Mechanisms, transfers may also take place using a derogation under Article 49 EU GDPR.

Law Enforcement Directive (LED)

1. **Appropriate safeguards** – these can be used where controllers have concluded that an appropriate level of protection for personal data exists in a third country or international organisation on the basis of a legally binding instrument or a case-by-case assessment. The LED itself does not set a threshold for what constitutes an appropriate level of protection, but the European Data Protection Board has defined it as an "essentially equivalent level of protection" to the LED.

2. A number of **'special circumstances'** that can be used in specific circumstances.

Received 7 May 2024