Understanding the risks to cross border transfer of personal data: EU-UK Data Adequacy

September 2023

EU-UK Data Adequacy

A report produced on behalf of the Department for the Economy by Dr Orla Lynskey; Dr Maria Helen Murphy and Dr Katherine Nolan with research assistance provided by Éadaoin Burns and Luben Roussev.

Contents

List of Abbreviations

ABBREVIATION	FULL TITLE
A29WP	Article 29 Working Party
AI	Artificial Intelligence
ALLEA	The European Federation of Academies of Sciences and Humanities
APPI	Act on the Protection of Personal Information, Japan
BCR	Binding Corporate Rules
CEO	Chief Executive Officer
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoC	Codes of Conduct
DAERA	Department for Agriculture, Environment and Rural Affairs of Northern Ireland
DCMS	The Department for Culture, Media and Sport
DPA	The Data Protection Act
DPC	Data Protection Commission, Ireland
DPDI (No 2) Bill	Data Protection and Digital Information (No 2) Bill
DPF	Data Privacy Framework
DPIA	Data Protection Impact Assessments

DPPEC	The Data Protection, Privacy and Electronic Communications Regulations
ECHR	European Convention on Human Rights
ECNI	Equality Commission for Northern Ireland
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EO 14086	Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence Activities
EU	European Union
FOI	Freedom of Information
FSB	Federation of Small Businesses
GATS	General Agreement on Trade in Services
GB	Great Britain
GDPR	General Data Protection Regulation
HR	Human Resources
ICO	Information Commissioner's Office
NI	Northern Ireland
NIHRC	Northern Ireland Human Rights Commission
NIRSRA	Northern Ireland Statistics and Research Agency
PNR	Passenger Name Record

PPC	Personal Information Protection Commission, Japan
RoI	Republic of Ireland
SA	Supervisory Authority
SCC	Standard Contractual Clauses
SCOTENS	The Standing Conference on Teacher Education, North and South
SIT	The Department for Science, Innovation and Technology
SME	Small and Medium Sized Enterprise
SoS	Secretary of State
SPS	Sanitary and Phytosanitary
TCA	The Trade and Cooperation Agreement
TFEU	The Treaty on the Functioning of the European Union
TUC	Trade Union Congress
UK	United Kingdom
UK GDPR	United Kingdom General Data Protection Regulation
US	United States of America
WP12	Article 29 Working Party, Working Document: Transfers of personal data to

	third countries: Applying Articles 25 and 26 of the EU data protection directive
WP237	Article 29 Working Party, Working Document: 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)
WP254	Article 29 Working Party, Adequacy Referential
WTO	World Trade Organisation

Executive Summary

Northern Ireland (NI) is in a unique position within the UK due to its shared border with the EU and its close economic, political, and societal links with the Republic of Ireland (RoI). Given this unique position, it is plausible to imagine that NI would be significantly affected by any impediments to the transfer of data from the EU to NI. At present, the unhindered flow of personal data from the EU to NI is facilitated by an EU adequacy decision. This decision of the European Commission recognises that individuals whose data are transferred from the EU to the UK are offered an essentially equivalent level of fundamental rights protection to that offered in the EU. This adequacy decision is, however, subject to a sunset clause and will end in June 2025. The European Commission should therefore begin its review of the decision by the end of next year.

The aim of this report is threefold. First, it seeks to ascertain the role and importance of data transfers from the EU to NI. Second, it examines whether there is a risk the UK will lose its adequacy status and assesses the likelihood of this outcome, in light of the changes proposed to UK data protection law by the Data Protection and Digital Information (No 2) Bill (the DPDI (No 2) Bill). Finally, it examines what mitigation measures might be available to data importers in NI in the event of a loss of adequacy and assesses their viability.

To inform the report's findings a detailed reading of the DPDI (No 2) Bill and its Explanatory Notes was conducted and the existing pre- and post-GDPR adequacy decisions of the European Commission were analysed. This research provided practical insights into how the Commission may respond to the legislative changes proposed in the UK. Furthermore, as there is a risk that a renewed adequacy decision might be challenged before the Court of Justice of the EU, relevant caselaw was examined to assess the likelihood of such a successful challenge. This research was complemented with some semi-structured

interviews with affected stakeholders (both on- and off-record) and a literature review. The key findings of the report are as follows.

The Significance of Data Adequacy for Northern Ireland

When considering the importance of adequacy for NI, it is imperative to consider its unique circumstances. A loss of adequacy would have significant and specific implications for NI due to its economic and social ties with the RoI. This report identifies three particularly important factors when assessing the specific impact of a loss of adequacy on NI. These are:

(i) the disproportionate impact of a loss of adequacy on SMEs;
(ii) the consequences of a loss of adequacy for all-Island initiatives in various sectors; and,
(iii) the effect a loss of adequacy may have on the ability of entities to comply with their Windsor Framework duties.

Risks to Data Adequacy Posed by the Data Protection and Digital Information (No 2) Bill

Our analysis of the DPDI (No 2) Bill identifies four key areas of change that could potentially threaten UK data adequacy. These are changes to data protection law related to:

i. **Independence and Political Influence**: Changes related to independence and political influence have the potential to threaten UK adequacy status. This is likely the most significant risk to adequacy contained in the DPDI (No 2) Bill.
ii. **Access to Effective Individual Remedies**: The dilution of the individual right to lodge a complaint in favour of a shift to more strategic enforcement has the potential to undermine the UK adequacy decision.

iii. **Onward Transfers of Personal Data**: The DPDI (No 2) provision for onward transfers is likely to be subject to intense scrutiny by the Commission. Additional assurances and safeguards aligned with EU standards are likely to be required.

iv. **Changes to the rights of individuals and other societal safeguards**: Taken individually, these changes are likely to be acceptable on the basis that the standard of adequacy is essential equivalence and not identical protection. That being said, the changes could be viewed as contributing to a general degradation in data protection rights and that could go against the UK in a holistic assessment of adequacy.

Mitigation Measures

A mitigation measure must be targeted to remedy the adequacy deficiency identified by the Commission or the CJEU. This contextual information is needed to identify an appropriate mitigation measure with confidence. Moreover, it follows from the CJEU's caselaw, that if alternatives to adequacy are used to facilitate data transfers to a place deemed inadequate, then the data exporter must conduct a contextual assessment to make sure these alternatives do not suffer from the same shortcomings. This means that a loss of adequacy status also impacts upon the application of other mitigation measures.

The following established mitigation measures were considered:

- **Partial adequacy decisions:** It is possible for the EU Commission to adopt tailored or partial adequacy decisions. These partial decisions allow the Commission to overcome impediments to an adequacy finding by introducing exceptions to the scope of the adequacy decision, adding supplementary conditions to the adequacy decision or by recognising adequacy on a partial geographic basis. This type of bespoke arrangement might be used to address some of the concerns with the DPDI (No 2) Bill, such as the risks from onward transfers or the changes to the rights of individuals. However, a partial adequacy decision is unlikely to address more systemic issues, such as concerns about the independence of the regulator.

- **Appropriate contractual safeguards:** The EU data protection framework allows for transfers of data to non-EU states lacking adequacy where the data exporter puts in place 'appropriate safeguards', including contractual mechanisms. The two main contractual mechanisms are SCCs and BCR. SCCs are model clauses that can be adhered to by data exporters and importers to ensure an appropriate level of data protection while BCRs are contractual provisions entered into by members of the same corporate group that serve the same purpose. These mechanisms are well-established and tested and offer a viable option for data transfers, particularly for entities with sufficient resources and data protection experience. The resources required to implement these contractual mechanisms is, however, a key disadvantage. A further disadvantage is that these mechanisms do not apply in a legal vacuum: the data exporter cannot ignore the wider legal context in which they apply and, following CJEU caselaw, must undertake an assessment of whether the level of protection offered in NI is appropriate. This contributes to the cost and uncertainty of using these contractual mechanisms.

- **An agreement between public authorities or bodies in the EEA and those in NI:** A further 'appropriate safeguard' that might apply in the absence of adequacy is an agreement between public authorities or bodies in the EEA and those in NI. This agreement should ordinarily be binding but non-binding agreements, such as memoranda of understanding, can be used if they have obtained the approval of the relevant supervisory authority (for instance, the Irish Data Protection Commissioner if the transfer is between a public authority in the RoI to a public authority in NI). The use of such agreements may be complicated by the question of whether NI public authorities and bodies have the legal capacity to enter into binding international agreements. Moreover, like other appropriate safeguards, the use of these agreements must take into consideration whether compliance with them can ensure essentially equivalent data protection in practice due to the laws in place in NI.

- **Derogations for specific situations:** EU data protection law does foresee derogations to the general rule that data can only be transferred to a non-EU entity offering an adequate level of protection. These include situations where the data subject is cognisant of the risks of the transfer but provides explicit consent; where data transfers are required for contractual purposes or for important reasons of public interest, amongst others. There remains some ambiguity about whether these derogations can be relied upon to facilitate frequent or larger scale data transfers and there are compliance costs associated with reliance on them. Nevertheless, for data importers to NI they may offer a viable and attractive option for data transfers in the absence of adequacy.

There are also a several more speculative or less well-established routes to facilitate data transfers, the feasibility of which we considered. These were:

- **Narrowing the definition of a data transfer:** It is possible to argue that no data transfer occurs where the data recipient in NI is already subject to the EU's GDPR because of its expansive territorial scope or because the transfer takes place internally within an organisation and does not involve any additional data controllers or processors. In both situations the logic would be that as the GDPR applies anyway, there is no need to provide an additional layer of protection by invoking the data transfer rules. The positions of relevant actors, such as the EDPB and the EU Commission, on these arguments are ambiguous and sometimes contradictory. This is therefore a higher risk option to facilitate data flows between the EU and NI than some of the others available.

- **New 'appropriate safeguards' to which the importer can adhere:** Codes of conduct (CoC) and certification mechanisms offer data importers the opportunity to prove their own compliance with EU data protection standards and to show they are trusted data importers. Where an entity in NI is not

already subject to the GDPR, they can only adhere to CoC with general validity. There must also be a CoC appropriate to the sector concerned available to the data importer. Certification schemes are more widely applicable but only one certification scheme has been recognised so far. Both require significant resources and capacity of the data importer. Moreover, like other appropriate safeguards, the data exporter will still need to assess whether compliance with the CoC or certification mechanism is itself sufficient for adequacy or whether supplementary measures are required.

- **Challenging the EU using international trade law:** It is possible that the EU's data transfer regime constitutes an unnecessary interference with free trade and violates existing international trade agreements. However, this is at best a medium-term solution as until such a claim is taken and upheld the EU adequacy rules will continue to apply. Moreover, the EU would find itself caught between compliance with two legal regimes – a compliance deadlock – and it is unclear how this deadlock would ultimately be resolved.

1 Introduction

While a reference to international data transfers tends to conjure up images of data flows between tech titans, the reality is that cross-border data flows form the backbone of many forms of economic, social and political activity these days. This is particularly so in Northern Ireland (NI) where there are close links with the UK and the Republic of Ireland (RoI). Post-Brexit, the rules under the EU General Data Protection Regulation (GDPR)[1] concerning data exports from the EU create new complications for NI operators. When data is transferred from an EU entity to a non-EU entity, then supplementary rules apply to the transfer. This is to ensure that the level of protection afforded to individuals under EU data protection law is not undermined or circumvented by the transfer of the data outside of the EU. Data flows between NI and the rest of the UK are not regarded as exports, and as such are not subject to any additional regulatory requirements. At present, data transfers from the EU to NI are facilitated by the existence of an EU adequacy decision, recognising that the UK offers an essentially

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

equivalent level of data protection to individuals as that found in the EU. However, this adequacy decision is subject to a sunset clause and will be reviewed by June 2025. Moreover, changes to the UK's data protection regime may affect this assessment.

The aim of this report is threefold. First, it seeks to ascertain the role and importance of data transfers from the EU to NI. Second, it examines whether there is a risk the UK will lose its adequacy status, and assesses the likelihood of this outcome, in light of the changes proposed by the UK's Data Protection and Digital Information (No 2) Bill (the DPDI (No 2) Bill). Finally, it examines what mitigation measures might be available to data importers in NI in the event of a loss of adequacy and assesses their practical viability. Before proceeding to the substantive analysis, it is necessary to clarify the scope of this report and to set out the methodology used to produce it.

1.1 Scope of the Report

This report is concerned with the potential loss of the UK's adequacy status as a matter of EU law. In other words, it is primarily concerned with a scenario where a NI importer receives data from the EU: the relevant data flow is therefore from the EU (including the RoI) to NI rather than from NI to the EU.

At present, the EU recognises the UK as adequate and the UK recognises the EU as such. However, as both the UK and the EU conduct separate adequacy assessments, it is entirely possible that the EU might change the UK's adequacy status while the UK continues to recognise the EU as adequate. In such a case, importing data from the EU would be subject to additional regulatory requirements while data exports to the EU might continue unhindered. Indeed, we might expect this to be the case as it is the UK law which is changing rather than that of the EU. Nevertheless, as this report implicitly highlights, adequacy assessments require a certain amount of political will, and it is possible that the UK might find grounds to withdraw the EU's adequacy status in this scenario. It is notable that it is the Secretary of State (SoS) that confers adequacy status on third countries and regions pursuant to the DPDI (No 2) Bill. A reciprocal loss of adequacy would complicate life for data controllers and processors

in NI even further. In such a scenario, both data exports from NI and data imports to NI would be challenged.

Irrespective of whether the UK revokes the EU's adequacy status in response to a loss of EU adequacy on its part, one might query whether EU data recipients might refuse to receive data transferred from data exporters in an 'inadequate' UK. This seems unlikely as there are no explicit requirements for data import found in the EU's GDPR. It might be argued that the import of poor quality data (inaccurate data or data of unverified provenance) might undermine the ability of an EU controller to comply with the GDPR's data quality principle[2], or the requirements of the EU AI Act where applicable.[3] However, this possibility might be discounted as remote.

Furthermore, while the European Commission's decision to grant the UK adequacy status might have been questioned on the grounds of the national security regime in place in the UK, this report does not revisit this initial assessment of the UK's adequacy. Moreover, although the DPDI (No 2) Bill does make changes to the data processing for intelligence and national security purposes (notably Clauses 21, 27 and 28), the compatibility of these changes with EU law is not examined in this report. There are concerning elements to these proposed amendments, for instance the expansion of the national security exemption and the possibility for the SoS to withhold information about what entities are designated as competent authorities for joint processing for intelligence purposes. These changes may not meet the 'essential guarantees' required by EU law for national security and law enforcement surveillance in third countries.[4] However, given the complexity of this area of law and the timeframe in which this report was concluded, such considerations are beyond its scope. It must be noted however that should the UK adequacy decision be challenged before the CJEU following the adoption of the DPDI (No 2) Bill the CJEU may look less favourably on

[2] Article 5(1)(d) GDPR.

[3] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021) COM/2021/206 final (AI Act), Article 10(3).

[4] Article 29 Working Party, Adequacy Referential, adopted on 27 November 2017, as last revised and adopted on 6 February 2018, WP 254 rev.01, 9.

the UK's national security and law enforcement processing than the Commission did in the original UK adequacy decision and it would also take the recent changes in the DPDI (No 2) Bill into account in assessing adequacy status.

While this report focuses on the potential implications of the DPDI (No 2) Bill for EU adequacy, it is worth noting that the Bill may also raise other legal issues of importance for NI. Data protection legislation cannot be entirely separated from underlying fundamental rights protections, as the legislation implements and is informed by fundamental rights, particularly the right to respect for private life and the right to protection of personal data. The potential for changes to fundamental rights instruments or standards applicable in the UK is therefore also relevant to the matter of adequacy. Article 2 of the Protocol on Ireland/Northern Ireland provides that the UK shall ensure that there is 'no diminution of rights' as set out in the Belfast/Good Friday Agreement. The preamble highlights that 'Union law has provided a supporting framework for the provisions on Rights, Safeguards and Equality of Opportunity of the 1998 Agreement'. The Belfast/Good Friday Agreement includes a commitment to the 'civil rights' of 'everyone in the community'. The UK Government also pledged to incorporate the ECHR into domestic law.[5] In an explainer on its post-Brexit commitment to rights in NI, the UK Government affirms its commitment to protecting the rights provided for in the Belfast/Good Friday Agreement as supported by the ECHR and acknowledges that EU law 'has formed an important part of the framework for delivering the guarantees on rights and equality set out in the Agreement'.[6]

---

[5] This was achieved with the passage of the Human Rights Act 1998. The Belfast/Good Friday Agreement was ambiguous regarding the necessity of RoI incorporation, but the RoI Government subsequently passed the ECHR Act 2003. This was influenced by the commitment to introduce measures that would ensure an equivalent level of protection of human rights across the island. Belfast/Good Friday Agreement: The Multi-Party Agreement; Maria Helen Murphy, 'Repealing the Human Rights Act: Implications for the Belfast Agreement' [2015] 26(3) King's Law Journal 335-347, 342.

[6] Explainer: UK 'Government Commitment to No Diminution of Rights, Safeguards and Equality of Opportunity in Northern Ireland' [2020] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/907682/Explainer__UK_Government_commitment_to_no_diminution_of_rights__safeguards_and_equality_of_opportunity_in_Northern_Ireland.pdf>.

In a report on the scope of Article 2 of the Protocol, the Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland[7] set out their working assumption that 'all EU law in force in NI on or before 31 December 2020 which underpins an ECHR right falls within scope of the non-diminution commitment in Protocol Article 2'.[8] The NIHRC and the ECNI specifically rely on data protection law as an example of an area of law that falls within the scope of Article 2. As reasoned by the Commissions, the right to protection of personal data constitutes a civil right under the Belfast/Good Friday Agreement and the protection of personal data afforded by the EU GDPR is underpinned by Article 8 ECHR.[9] Accordingly, if the DPDI (No 2) Bill becomes law and is considered to constitute a diminution of rights, a potential challenge could be made in NI on the basis of Article 4 of the Withdrawal Agreement and Article 2 of the Protocol. A legal analysis of the viability of such a challenge does not fall within the scope of this report.

Finally, this report was concluded in a tight timeframe and does not pertain to be exhaustive. Rather, it serves to highlight the particular significance of adequacy for NI; the main potential challenges to adequacy because of the proposed data protection law reform; and the most viable alternatives to adequacy for data importers in NI should the UK lose its adequacy status.

1.2 Methodology

The research conducted for this report was primarily desk-based doctrinal legal research. This involved, amongst others:

---

[7] Two bodies were set up under the Belfast/Good Friday Agreement. The Protocol provides that the UK will continue to facilitate the work of these bodies set up under the Belfast/Good Friday Agreement in addition to the work of the Joint Committee of representatives of the Human Rights Commissions of Northern Ireland and Ireland.

[8] The Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland, Working Paper: 'The Scope of Article 2(1) of the Ireland/Northern Ireland Protocol' [2022] 13.

[9] The Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland, Working Paper: [2022] 13.

- A close reading of the provisions of the DPDI (No 2) Bill and its Explanatory Notes;
- An examination of the relevant caselaw of the CJEU to inform understanding of the Court's approach to cross-border data transfers;
- A detailed analysis of the 19 relevant adequacy decisions adopted by the European Commission both pre- and post-GDPR to gain practical insights into how the Commission may respond to the UK's proposed legislative changes;
- A literature review of existing academic and policy publications relevant to the analysis.

To gain a better understanding of the extent and significance of data flows between the EU and NI, several semi-structured interviews were conducted with volunteers from the NI Civil Service, non-statutory bodies and research organisations. Some of the interviewees provided consent to insights from their interviews being included in this report while others preferred for their interviews to provide background context for the report and to remain off-record.

Finally, no independent economic research was conducted for the purposes of this report. Our assessment of the economic implications of adequacy for NI is informed by a literature review conducted by an economist for these purposes.

2 The Legal, Political and Economic Context

2.1 Introduction

NI occupies a unique position within the United Kingdom (UK) as, amongst other factors, the only constituent part sharing a land border with an EU Member State. Prior membership of the European Union (EU) and the Single European Market facilitated the free movement of goods, capital, services and people between the UK and the rest of the EU, including across the border between NI and the RoI (the latter complementing the existing free movement of people under the Common Travel Agreement). While not one of the four fundamental freedoms, membership of the EU facilitated seamless data flows between the UK and other Member States based on harmonised data protection standards, with significantly less complication than those facing non-EU States (or 'third countries' in EU terminology). To effectively navigate the transition from being a Member State of the EU to a third country, and to fully understand the potential implications for data transfers, it is important to consider the specific legal, political, and economic context in NI.

The particular challenges of Brexit arising in the Northern Irish context were recognised by both the UK and the EU from the earliest point of the withdrawal process. In her Article 50 notification letter to then President of the EU Council, Donald Tusk, former Prime Minister, Theresa May, stated that 'we must pay attention to the UK's unique relationship with the Republic of Ireland'. She highlighted the importance of avoiding a hard border and ensuring that 'nothing is done to jeopardise the peace process in Northern Ireland, and to continue to uphold the Belfast Agreement.'[10] Notably, the joint political declaration accompanying the Withdrawal Agreement explicitly recognises the importance of data flows and data protection. In Part I(I)(B) of the political declaration, directly below the provision for 'core values and rights'[11], the declaration states that

[10] Theresa May, 'Prime Minister's Letter to Donald Tusk Triggering Article 50' (Article 50 of the Treaty on the Functioning of the EU [2017] <https://www.gov.uk/government/publications/prime-ministers-letter-to-donald-tusk-triggering-article-50/prime-ministers-letter-to-donald-tusk-triggering-article-50> .

[11] Political Declaration (EC) (2019/C 384 I/02). which notes that the 'future relationship' should incorporate the UK's 'continued commitment to respect the framework' of the ECHR.

'[i]n view of the importance of data flows and exchanges across the future relationship, the Parties are committed to ensuring a high level of personal data protection to facilitate such flows between them.'[12]

Similarly, the Protocol on Ireland/Northern Ireland, an integral part of the Withdrawal Agreement, expressly acknowledges the unique challenges that the UK withdrawal from the EU raised for the island of Ireland and acknowledges the need for a 'unique solution' to address the 'unique circumstances'.[13] The Protocol recognises that cooperation between NI and RoI is a central part of the Belfast/Good Friday Agreement. In addition to setting out the objectives of preventing a hard border and maintaining the 'necessary conditions for continued North-South cooperation', the Protocol also underlines the shared aim of 'avoiding controls at the ports and airports of Northern Ireland'.[14] The complexity is clear from the qualifying language of the Protocol that states this aim is to be pursued 'to the extent possible in accordance with applicable legislation and taking into account their respective regulatory regimes as well as the implementation thereof'.[15]

The Protocol on Ireland/Northern Ireland helped prevent the creation of a hard border – including avoiding the imposition of physical infrastructure or related checks and controls – on the island of Ireland.[16] An unfortunate consequence of this, however, was the creation of heightened trade barriers between NI and the rest of the UK. As

---

[12] The declaration goes on to refer to the adequacy framework and the EU's commitment to begin the adequacy assessment of the UK's data protection regime 'as soon as possible' after the completed withdrawal of the UK from the EU.

[13] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2020] OJ L 29/7 (Withdrawal Agreement).

[14] Joint Declaration No 1/2023 of the Union and the United Kingdom in the Joint Committee established by the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community of [2023] OJ L102/87. Another notable point is that the Protocol also specifies that it should not impede the UK's ability to ensure 'unfettered market access for goods moving from Northern Ireland to the rest of the United Kingdom's internal market'.

[15] ibid.

[16] Withdrawal Agreement (n 13); Emma Kerins, Shane Conneely and Michaela Reilly, 'The Case for Enhanced Cross Border Co-Operation' [2020] The Journal of Cross Border Studies in Ireland 149.

described in a report from the House of Lords European Affairs Committee, this shift resulted in an increase in bureaucratic processes, resource allocation, costs, and delivery timelines for businesses engaged in trade between GB and NI.[17] While a hard border between RoI and NI has been avoided, a 'soft-border' remains necessary to account for the new UK-EU relationship and the potential for diverging regulatory standards, the Protocol allows for cross-border trade in goods to continue without checks at the RoI-NI border. The Protocol on Ireland/Northern Ireland has since been amended by the Windsor Framework[18] which a recent report from relevant House of Lords Sub-Committee described as 'the latest attempt to manage the implications of Brexit for Northern Ireland.'[19] A key part of the Windsor Framework is a system where UK-traded goods intended for sale in NI rather than the EU can be moved in a streamlined fashion using a 'green lane' system, reducing the paperwork and checks required for internal trade between the UK and NI while maintaining third country requirements for goods intended for onward travel to the EU (including to the RoI). It should therefore remove internal UK trade barriers, including 'third country' processes such as officially-signed certificates for individual food products and customs declarations for consumer parcels.[20] The Windsor Framework acknowledges that to maintain unencumbered access for NI goods to the EU single market, NI must continue to align with EU policies. To ensure these policies are adhered to in practice, while facilitating 'green-lane' UK-NI trade, the UK and the EU agreed to new data-sharing arrangements to assist with the monitoring and management of risks with the aim of protecting the integrity of the EU and UK internal markets.[21] The importance of data-sharing in this agreement highlights the integral role of data flows in all modern trade

[17] House of Lords: European Affairs Committee, 'Report from the Sub-Committee on the Protocol on Ireland/Northern Ireland: Follow-up Report' [2022] HL Paper 57, 3.
[18] Joint Declaration No 1/2023 (n 14).
[19] House of Lords: European Affairs Committee, 'Report from the Sub-Committee on the Protocol on Ireland/Northern Ireland: The Windsor Framework' [2023] HL Paper 237, 5.
[20] HM Government, 'The Windsor Framework: A New Way Forward Presented to Parliament by the Prime Minister and Minister for the Union by Command of His Majesty' (2023) CP 806, 8 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138989/The_Windsor_Framework_a_new_way_forward.pdf>.
[21] ibid, 4.

and the success of the Windsor Framework will require consideration of data protection and planned mechanisms for data transfer.

2.2 Economic Costs of Losing Adequacy Status

The free flow of data between NI and the EU has many economic benefits, including the boosting of 'productivity and growth, fostering trade, innovation and entrepreneurship', as well as higher trust and higher interoperability of legal frameworks.[22] Furthermore, the free flow of information across borders is supporting an increasing range of economic activities. These benefits increase the level of cross-border transactions.[23] Cross border data flows are considered 'essential' to the conduct of international trade and commerce.[24] Data flows enable companies to 'transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation'.[25] As a result, cross border data flows increase productivity and enable innovation.[26] The operational impacts of data transfer restrictions also extend beyond the immediate effect on trade, as cascading economic benefits associated with the free flow of data may also be lost. As noted by DigitalEurope the free movement of data without restriction facilitates many activities including the:

> moving of HR information from a subsidiary to a parent company, transferring health data for ground-breaking research, or simply being able to use the perfect application for the tasks you need to do. Hampering the data flows behind these

[22] Vincenzo Spiezia and Jan Tscheke, 'International Agreements on Cross-Border Data Flows and International Trade: A Statistical Analysis' [2020] OECD Science, Technology and Industry Working Papers 2020/09, 6 <https://doi.org/10.1787/b9be6cbf-en.>.
[23] ibid.
[24] Rachel Fefer, 'Data Flows, Online Privacy, and Trade Policy' (Congressional Research Service 2020) R45584 1.
[25] ibid.
[26] ibid.

business decisions has a negative impact on all companies' economic prospects.[27]

Research indicates that there is significant economic value to maintaining the current adequacy status. The economic costs of a lack of an adequacy decision include reduced market access, trade, investment, and restricted 'access to digital goods and services'.[28] The disadvantages of a loss of adequacy highlight the economic benefits of the current adequacy decision between the UK and EU. Specifically, countries who have received EU adequacy exhibit an increase in digital trade between 6-14%, representing a trade cost reduction of up to 9%.[29] Some refer to the *club effect* of data adequate countries, with 'approximately 7 percent of digital value-added trade shifted towards the network of countries with adequacy away from countries without adequacy'.[30]

Further, the prospective economic cost of a loss of adequacy is significant. The aggregate cost to UK firms of a no adequacy decision is estimated to be between £1 billion and £1.6 billion.[31] Wider economic impacts include reduced EU-UK trade, reduced UK investments and the relocation of business functions outside the UK.[32] Overall, these economic implications of losing the adequacy decision have the potential to undermine the competitiveness of NI and the wider UK, particularly in key service areas that are highly dependent on cross border data flows including banking, retail and hospitality. For example, 'half of all trade in services is enabled by seamless

---

[27] Digitaleurope, 'Data Flows and The Digital Decade' 3. Available at <https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf>.

[28] Andreas Aktoudianakis, 'Data Adequacy post-Brexit: Avoiding disruptions in cross-border data flows' European Policy Centre [2015] 83-84 <https://www.epc.eu/content/PDF/2020/10_Data_adequacy.pdf>.

[29] Martina Francesca Ferracane, Bernard M Hoekman, Erik Van Der Marel, and Filippo Santi, 'Digital trade, data protection and EU adequacy decisions'(EUI, RSC, Working Paper, 2023/37) Global Governance Programme-505, European Centre for International Political Economy (ECIPE) [2023] 1 <https://hdl.handle.net/1814/75629>.

[30] ibid 7.

[31] Duncan McCann, Oliver Patel and Javier Ruiz, 'The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure An EU Data Adequacy Decision' (2020) New Economics Foundation UCL European Institute 2 <https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf>.

[32] ibid 35.

cross-border data flows'.[33] Saluste states that with adequacy agreements, 'companies face less burden, as there is an authority in the third country standing out for their interests, it is less costly for them as they do not need to negotiate or renegotiate contractual clauses with their business partners to comply with the GDPR'. For example, 'renegotiating contracts is costly, lengthy, and possibly with certain trade-offs'.[34]

Due to the economic and societal connections between NI and RoI, the ability to transfer data across the border is particularly important. While the Protocol – as amended by the Windsor Framework – sets out to protect continued free movement of goods between NI and RoI while maintaining the integrity of the UK internal market; the adequacy decision of the EU Commission facilitates the continued free flow of data from the EU to the UK. For NI, this is not only essential for continued trade with the EU but it plays an integral role in facilitating the continued cross-border interactions that have significant value for those in NI and the RoI. There are concerns about the impact of a loss of adequacy and the consequences for organisations who may not be adequately prepared to make the legal arrangements necessary to continue to receive personal data from the EU.[35]

The interconnections between the economies and societies of NI and the RoI means that a loss of adequacy status would entail specific implications and challenges for NI. The economies of NI and the RoI are increasingly integrated, as demonstrated by recent evidence. While cross-border economic activity between NI and RoI has previously been characterised by 'fragmentation' and 'poor integration', there has been

[33] Oliver Patel and Nathan Lea, 'EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?' [2019] UCL European Institute 3. Available at <https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no_deal_updated.pdf>.

[34] Maarja Saluste, 'Adequacy Decisions: An Opportunity for Regulatory Cooperation on Data Protection?' [2021] 4. Available at: <https://respect.eui.eu/wp-content/uploads/sites/6/2021/01/Saluste_Adequacy-decisions-Jan18-2021_RESPECT_final.pdf>.

[35] Patel and Lea, 'EU-UK Data Flows, Brexit and No-Deal' (n 33) 2.

significant change since the 1990s.[36] Now, NI and RoI have strong economic links as evidenced by statistics from the Northern Ireland Statistics and Research Agency that report the total value of Northern Irish sales to RoI as amounting to £5.2 billion in 2021, up from £4.2 billion in 2020.[37] In December 2022, NIRSRA noted that sales to RoI 'are at their highest levels on survey record'.[38] Kerins, Conneely and Reilly have noted that the two jurisdictions have a 'lower than typical border effect' due to commonalities that help to facilitate trade and this has led to increased prosperity for traders on both sides of the border and positive secondary effects in both economies.'[39]

While there is no economic data that precisely quantifies the cost of a loss of adequacy on NI, existing empirical work suggests significant consequences. The qualitative semi-structured interviews conducted for this study identified further specific implications a loss of adequacy would have for NI. One such example concerns cross-border workers: a significant number of people live in a different jurisdiction to which they are employed.[40] The Centre for Cross Border Studies estimates that 23,000-30,000 people are cross-border workers. This group of people are one of the key stakeholder groups who will be negatively impacted by an inadequacy decision. For example, 'simple matters like payroll' will be negatively impacted.[41] The issue of payment and pensions will impact on a host of data controllers, ranging from public sector providers (for instance, the payment of teachers or medical workers) to private operators (such as factory owners or SMEs such as shopkeepers). This issue was raised in interviews. Whether such pensions and payroll payments could be facilitated

---

[36] David Phinnemore and Katy Hayward, 'UK Withdrawal (Brexit) and the Good Friday Agreement: A Study for the AFCO Committee [2017], 22; Kerins et al, 'The Case for Enhanced Cross Border Co-Operation' (n 16) 152.

[37] Northern Ireland Statistics and Research Agency, 'Northern Ireland Economic Trade Statistics 2021' [2022] <https://datavis.nisra.gov.uk/economy-and-labour-market/northern-ireland-economic-trade-statistics-2021.html#5_Background_Notes>.

[38] ibid.

[39] Kerins et al, 'The Case for Enhanced Cross Border Co-Operation' (n 16) 150.

[40] Emma Dellow-Perry, 'The UK's Exit from the EU – Data Protection, Adequacy and Divergence' (Research Matters, 14 April 2021) <https://www.assemblyresearchmatters.org/2021/04/14/the-uks-exit-from-the-eu-data-protection-adequacy-and-divergence/>.

[41] ibid.

by reliance on consent in the absence of adequacy will be considered below. Moreover, many more fluid but less structured connections exist. For example, individuals may socialise, shop, and avail of services, including medical services, either side of the border. The flow of people and information for the purposes of education provides another example, with cross-border student mobility being found to provide economic, social, and cultural benefits for those North and South of the border.[42]

2.3 Considering Northern Ireland and its Unique Circumstances

There is a risk that discussions about data transfers can be dominated by the issues facing specific sectors, particularly those related to technology services. While efficient data transfer mechanisms are, of course, essential for the operation of these businesses, companies of all sizes and in all sectors can be affected by restrictions on cross-border data flows.[43] Notwithstanding that the loss of data adequacy would have significant consequences for the services sector, other sectors, including manufacturing, are now also heavily reliant on data and would be negatively impacted by restrictions on data flows.[44] Indeed, EU-UK data flows are vital for virtually any business with customers, suppliers or operations in the EU.[45] Accordingly, the protection of seamless data transfers from the EU, particularly the RoI, is important for continued trade growth in NI.[46]

Nevertheless, in assessing the specific impact of a loss of adequacy on NI, three factors should be highlighted: (i) the disproportionate impact of a loss of adequacy on SMEs; (ii) the consequences of a loss of adequacy for all-Island initiatives in various

---

[42] Billy Bennett and Simon Stephens, 'Reflections on the Provision of Higher Education through Cross Border Partnerships' [2020] The Journal of Cross Border Studies in Ireland 21 169, 170.
[43] Digitaleurope, 'Data Flows and The Digital Decade' (n 27) 4.
[44] ibid 3.
[45] Patel and Lea, 'EU-UK Data Flows, Brexit and No-Deal' (n 33) 2.
[46] According to the Central Statistics Office, goods exports from Northern Ireland to Ireland grew by €1,310 million to €5,354 million in 2022 (an increase of 32% from 2021) and goods imports to Northern Ireland from Ireland increased by €1,177 million to €4,942 million (an increase of 31% from 2021). Central Statistics Office, 'Goods Exports and Imports December 2022', (February 2023), 150.

sectors; and (iii) the effect this may have on the ability of entities to comply with their Windsor Framework legal duties.

(i) The disproportionate impact on SMEs

SMEs are particularly at risk in the event of a loss of adequacy status.[47] Patel and Lea note that the costs arising from the disruption caused by a no adequacy agreement will be particularly challenging for SMES who do not have the 'money, resources or expertise to deal with these new compliance burdens'.[48] Chander suggests that 'the effects of data inadequacy will fall disproportionately on smaller companies.[49] In the event of a loss of adequacy, such small businesses would also incur opportunity costs. For example, resources those businesses would have been 'free to spend to meet the requirements of the business by, for instance, investing in new equipment, staff, or processes', would need to be channelled into 'compliance activities' in order to mitigate EU-UK data flow disruption.[50] It has been recommended that the Government 'set aside funds to ensure that struggling UK businesses, especially small and medium enterprises (SMEs), can afford to comply with the new requirements', if they were to present themselves.[51]

[47] Patel and Lea, 'EU-UK Data Flows, Brexit and No-Deal' (n 33) 2; Ferracane et al, 'Digital trade, data protection and EU adequacy decisions' (n 29) 8; Anupam Chander, 'Is Data Localization a Solution for Schrems II?' [2023] 23 Journal of International Economic Law 771; McCann et al, 'The Cost of Data Inadequacy' (n 31) 20.

[48] Patel and Lea, 'EU-UK Data Flows, Brexit and No-Deal' (n 33) 12.

[49] Chander, 'Is Data Localization a Solution?' (n 47); see also Ferracane et al, 'Digital trade, data protection and EU adequacy decisions' (n 29) 8.

[50] McCann et al, 'The Cost of Data Inadequacy' (n 31) 25

[51] ibid 3.

While the success of SMEs is vital for the health of all the UK economy – accounting for 99.9% of businesses, 61% of total employment, and 51% of turnover[52] – the economy in NI is particularly exposed to any threat a loss of adequacy may pose to SMEs. In March 2023, the vast majority of businesses in NI (89% or 70,795) were recorded as being micro-businesses of less than ten employees. 42 per cent of businesses in NI (33,645) had a turnover of less than £100,000, and just 12 per cent (9,315) had a turnover greater than £1 million.[53] A 2016 report by FSB found that SMEs accounted for 75% of private sector turnover in NI and for more jobs than large enterprises and the public sector combined. As pointed out by the report, as 'a proportion of the economy, this is significantly greater on both these measures than the equivalent in the UK as a whole, making the protection and promotion of SMEs in Northern Ireland even more important'.[54] In light of this, it is particularly important to be aware of the potentially disproportionate effects that a loss of adequacy may have on the NI economy and efforts should be made to understand the experience and perspectives of those stakeholders most likely to be affected.

(ii) The impact on all-Island initiatives in various sectors

Both the UK Government and the European Commission have publicly acknowledged the importance of responding 'to the everyday issues faced by people and businesses in Northern Ireland' and 'supporting and protecting the Good Friday or Belfast

[52] Department for Business, Energy and Industrial Strategy, 'Business Population Estimates for the UK and Regions 2022: Statistical Release (HTML)' (GOV.UK) <https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html>.

[53] Northern Ireland Statistics and Research Agency, 'Inter Departmental Business Register' (<https://www.nisra.gov.uk/statistics/business-statistics/inter-departmental-business-register>; Department for the Economy, 'Northern Ireland Business; Activity, Size, Location and Ownership, 2023.' 22 June 2023, <https://www.economy-ni.gov.uk/news/northern-ireland-business-activity-size-location-and-ownership-2023>.

[54] FSB, Business Support in Northern Ireland [2016] https://www.fsb.org.uk/resources-page/business-support-in-northern-ireland.html.

Agreement in all its parts.'[55] Kerins, Conneely and Reilly have noted that while the Protocol was designed to protect the Belfast/Good Friday Agreement and the peace process, it may not be possible to 'fully mitigate many of the risks associated with Brexit'.[56] Data protection and free data flow play an important role in facilitating continued post-Belfast/Good Friday Agreement cooperation initiatives between NI and the RoI. Examples of all-island initiatives in the areas of health and research serve to illustrate this point.

North-South cooperation in health represents one of the 'relative success stories' in cross-border collaboration since the Belfast/Good Friday Agreement.[57] Significant actions have included the establishment of an All-Island Congenital Heart Disease Network by the Ministers for Health of both jurisdictions to provide specialist cardiac services for all children on the island of Ireland. As part of this, paediatric cardiac surgery is offered to children from NI at Children's Health Ireland at Crumlin.[58] Other examples include the building of a radiotherapy centre designed to serve a population of 500,000 people on both sides of the border and the establishment of a cross-border emergency cardiology service at Altnagelvin hospital in Derry.[59] These services require the exchange of personal data, including the exchange of special category health data which demands a higher level of protection.

---

[55] The changes brought about by the Windsor Framework were designed in pursuit of these common aims. The Windsor Framework was described as restoring 'the balance of the Belfast (Good Friday) Agreement by fundamentally recasting arrangements in three key areas: restoring the smooth flow of trade within the UK internal market by removing the burdens that have disrupted East-West trade; safeguarding NI's place in the Union by addressing practical problems affecting the availability of goods from Great Britain, and the ability of NI to benefit from UK-wide tax and spend policies; and addressing the democratic deficit that was otherwise at the heart of the old Protocol.' Windsor Political Declaration by the European Commission and the Government of the United Kingdom https://commission.europa.eu/system/files/2023-02/political%20declaration.pdf.

[56] Kerins et al, 'The Case for Enhanced Cross Border Co-Operation' (n 16) 150.

[57] Andy Pollak, 'North-South Cooperation on Healthcare during a Time of Corona Virus' [2020] The Journal of Cross Border Studies in Ireland 63, 63.

[58] Editorial Staff, 'Two New Professors of Paediatric Cardiology for All-Island Network' (Irish Medical Times, 28 January 2021) <https://www.imt.ie/news/two-new-professors-paediatric-cardiology-island-network-28-01-2021/> .

[59] Pollak , ' North-South Cooperation on Healthcare' (n 57) 63–64.

Notably, the Irish Department of Health has made representations to the Seanad Special Select Committee on the Withdrawal of the UK from the EU regarding the stated intention of the UK government to modify its data protection regime. In the Final Report on the Impacts of Brexit, representatives from the Irish Department of Health expressed concern about the potential for UK deviation from the framework as it would 'fundamentally impact' health, banking, trade, commerce, and 'service–to–service co-operation'.[60] Representing the Irish Department of Health, Muiris O'Connor noted:

> We made hundreds of data-sharing agreements. All organisations, on a cross-border basis had to do these data sharing agreements as a fallback in case the adequacy decision did not come through. I do not want us to go back there. The adequacy decision is what supports best international co-operation in health and right across other areas.[61]

It is not only in clinical contexts that this cooperation is vital. The Institute of Public Health, setup in 1998 just prior to the Belfast/Good Friday Agreement, plays an important role in the development of public health policies in NI and the RoI. The Institute is a north-south public agency with offices in Belfast and Dublin, which is jointly funded by health authorities in both jurisdictions. Its primary remit is to provide guidance on matters of health policy, including equity of health, mental health and wellbeing including issues such as alcohol consumption or smoking. Its work typically involves policy analysis, evidence synthesis and secondary analysis of data, however, it occasionally engages in primary data collection, for instance when conducting surveys of the views of service users and health professionals on a matter of policy. Yet, even without much primary data processing, the very operation of cross-border bodies such as the Institute of Public Health is complicated by any loss of adequacy.[62]

---

[60] The Seanad Special Select Committee on the Withdrawal of the UK from the EU, 'Final Report on the Impacts of Brexit', December 2021, 34.
[61] ibid.
[62] Interview with Adam McCune, Director of Communications and IT, Institute of Public Health.

Particular challenges also arise in the area of research. For instance, Stranmillis University College, Belfast, a small HEI with a particular focus on teacher education, has 180 members of staff. Its academics are active researchers who, because of funding made available for North-South initiatives following the Belfast/Good Friday Agreement, engage in many joint research projects involving children and researchers in the RoI. For instance, SCoTENS, the Standing Conference on Teacher Education North and South, has partnered with the Shared Island Unit at the Irish Department of an Taoiseach to offer funding with a broad focus on 'teaching and learning'. These projects are explicitly required to ensure 'extensive communication and collaboration opportunities between the various stakeholders both North and South'.[63] This initiative complements the existing annual seed funding that SCOTENS offers which has funded 126 projects since it was established in 2003. Proposals for these projects must be North-South partnerships, and the sums allocated are typically in the region of £3,000 to £6,000.[64] Such funding was deemed to be particularly important for early career researchers to gain experience of project management and coordination in a lower-risk environment.[65] Research projects such as these entail primary data collection, such as observational analysis of children in nursery or classroom settings. At present, adequacy allows for the seamless sharing of such data between partner research institutions in NI and RoI. However, in the absence of adequacy, small institutions like Stranmillis University College would not have the resources needed to manage the additional administrative burden of cross-border data flows at scale.[66]

(iii) The ability to comply with the legal requirements of the Windsor Framework

The Windsor Framework ensures that NI remains aligned with the EU Single Market rules for goods and gives an oversight role for compliance with these rules to the

[63] Shared Island/SCoTENS, 'Second call for funding applications', available at: https://scotens.org/call-for-funding-applications/.
[64] SCoTENS, 'Seed funding scheme', available at https://scotens.org/seed-funding-scheme/.
[65] Interview, Mark Shields, Stranmillis University College, Belfast
[66] ibid.

CJEU.[67] However, it also tackles the 'border in the Irish Sea' by permitting the partial disapplication of EU rules for goods where their final destination is NI. Goods produced in NI and intended for onward transfer to the EU, rather than elsewhere in the UK, continue to benefit from privileged status (unhindered access to the EU internal market) but must comply with EU regulatory requirements. Seamless data transfers form an integral part of this compliance picture, even in industries that would not typically be associated with personal data processing. One such example is agriculture where extensive sanitary and phytosanitary (SPS) regulation is in place to protect human, animal and plant life. In determining what goods are at risk of onward transfer to the EU from the UK through NI, the Joint Committee tasked with this assessment pays particular attention to goods subject to SPS checks.[68]

EU law provides for traceability requirements for livestock as part of disease control and enforcement measures. Livestock keepers must ensure that an animal has a correct ID and complete relevant movement documents and registers. Such documentation forms part of a wider DAERA system that ensures the birth to death traceability of animals. Traceability is critical to confidence in the supply chain and is amongst the reasons why an all-island animal health strategy was agreed in 2010.[69] Given the trade in livestock between NI and RoI such traceability also entails transfers of data from the EU to NI. At present, interoperable cross-border systems are in place to facilitate the transfers of data needed for traceability. A loss of adequacy would render practical compliance with such traceability requirements more cumbersome and costly, if not impossible, therefore impeding NI's ability to meet the requirements of the Windsor Framework.

[67] CRG Murray and Niall Robb, 'From the Protocol to the Windsor Framework' (2023) Northern Ireland Legal Quarterly 1, 2.
[68] ibid, 6.
[69] Ray Ryan: Irish Examiner, 'Ministers agree on all-island animal health and welfare strategy', 3 April 2010. <https://www.irishexaminer.com/business/arid-20116270.html>.

In sum, the potential costs of a loss of adequacy status for NI include jeopardising full participation in all-island and cross-border initiatives; rendering compliance with Windsor Framework legal requirements more cumbersome; increasing costs for public authorities and businesses, in particular SMEs; and disruptions to the day-to-day lives of cross-border workers and residents.

3 The EU Law Legal Framework

3.1 The GDPR

The GDPR is the primary piece of EU data protection legislation, which contains the main rules concerning data protection in the EU and creates an enforcement framework to oversee its application, led by national supervisory authorities in each Member State. One of the objectives of the GDPR is to promote the free flow of personal data within the EU. In line with classic liberalisation logic, the GDPR provides for substantive alignment of the data protection laws of EU Member States to protect fundamental rights, in particular data protection.[70] As a result of this substantive fundamental rights alignment, the free movement of personal data within the EU should not be impeded or prohibited based on fundamental rights concerns.[71] However, this liberalisation logic does not automatically extend to non-EU states whose laws cannot be assumed to align substantively with those of the EU. As a result, the GDPR distinguishes between data flows within the EU (where an adequate level of data protection is assumed in all EU Member States) and data transfers to outside of the EU (where such adequacy must be established).

[70] Article 1(2) GDPR.
[71] Article 1(3) GDPR.

Chapter V GDPR sets out specific rules that must apply where data is transferred from an EU Member State to a non-EU State (or third-country in EU law terminology).[72] The general principle underpinning these rules is one of anti-circumvention: personal data can only be transferred out of the EU when this transfer would not undermine the level of fundamental rights protection of natural persons afforded by the GDPR.[73] Chapter V sets out the terms on which transfers can be undertaken to achieve this anti-circumvention aim. Specifically, it provides for three mechanisms to facilitate international data transfers: (i) transfers based on adequacy decisions, (ii) transfers subject to appropriate safeguards and (iii) derogations for specific situations.

(i) Transfers Based on Adequacy Decisions

The European Commission has the power to designate a third-country, territory, sector or international organisation as 'adequate'. This indicates that an adequate level of fundamental rights protection exists when data is transferred to this place and no further authorisation is needed. The place concerned is treated in practice as equivalent to an EU Member State. Thus an adequacy decision is the most comprehensive transfer mechanism, requiring the least from data exporters and importers by way of compliance and enabling the broadest range of transfers.

In order to assess adequacy the Commission must take into account not only the data protection and privacy frameworks in that place but also factors including respect for the rule of law and human rights, legislation concerning law enforcement and national security, the rules on onward data transfers and the countries international data protection commitments.[74] In principle, the Commission must take into consideration caselaw as well as legislation in the third country as well as whether effective administrative and judicial remedies exist for individuals. Data protection compliance

[72] EEA States are treated as equivalent to EU Member States for the purposes of Chapter V. EU Commission, 'Rules on International Data Transfers', <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en>.
[73] Article 44 GDPR.
[74] Article 45(2)(a) and (c).

must be subject to oversight by an independent supervisory authority, which must function effectively and have adequate enforcement powers.[75]

Formally, adequacy is recognised in an implementing act of the European Commission which, in the GDPR era, should provide for periodic adequacy review, at least every four years. Moreover, the Commission is under an ongoing obligation to monitor developments that might negatively impact upon adequacy.[76] Where it reaches the conclusion that adequacy is no longer ensured, it must adopt an implementing act that – to the extent necessary – repeals, amends or suspends the adequacy decision. Where urgent these implementing acts may have immediate effect.[77] However, ordinarily the Commission should engage in consultations to remedy the deficiencies jeopardising adequacy status. Such obligations apply to adequacy decisions adopted under the GDPR's predecessor framework – Directive 95/46 EC – as well as under the current regime. At present, as detailed further below, only a small number of adequacy decisions have been adopted. These are publicised on the Commission's website.

(ii) Transfers Subject to Appropriate Safeguards

In the absence of an adequacy decision, the GDPR provides for data transfers where *appropriate safeguards* are put in place and the data subject is provided with enforceable rights and effective legal remedies. The most well-known of these safeguards are model contracts or 'standard contractual clauses' (SCCs), which must be adopted or approved by the European Commission. However, additional safeguards deemed appropriate include approved codes of conduct (CoC) and certification mechanisms as well as legally binding and enforceable instruments between public authorities or bodies. Where authorised by the relevant national data protection regulator, some additional measures might be deemed appropriate. These are contractual clauses between the relevant personal data exporter and recipient and provisions in administrative arrangements between public authorities which include

[75] Article 45(2)(b).
[76] Article 45(4) GDPR.
[77] See procedures found in Article 93(2) and (3) GDPR.

enforceable and effective data subject rights, and which are approved by a data protection authority rather than the Commission.

Where there is a group of companies engaged in joint economic activity, they can adopt a set of binding corporate rules (BCRs) that act as an 'appropriate safeguard' for data transfers within the corporate/organisational group. Although binding corporate rules are considered an appropriate safeguard, the GDPR specifies the formal conditions that BCRs must meet in a separate provision. These rules must bind every member of the corporate group and give individuals enforceable rights. Such rules require the prior approval of the competent national data protection regulator. Moreover, these rules must be externally binding; contain a complaints procedure and contain mechanisms to verify compliance.

(iii) Derogations for Specific Situations

Article 49 GDPR is entitled 'derogations for specific situations'. This provision helps to enable certain data transfers in the absence of an adequacy decision or appropriate safeguards. These include where the data subject has explicitly consented, having been informed of the possible risks of the transfer; where the transfer is necessary for the performance or conclusion of a contract or to protect the data subject's vital interests and where necessary for reasons of public interest or in relation to legal claims. Article 49(1) also allows for data transfers where none of these conditions are fulfilled but the transfer is not repetitive and concerns only a limited number of data subjects whose rights do not override the compelling legitimate interests of the controller in the transfer. The controller must also ensure that suitable safeguards are in place.

It is assumed that these three options were hierarchical: 'if an adequacy decision has been issued then that should be relied on; if not, then appropriate safeguards should

be used; and only if neither of these legal bases is available should the derogations be relied on'.[78]

3.2 The Jurisprudence of the Court of Justice of the EU

Data protection law has been at the centre of some of the CJEU's most notable jurisprudence, particularly since 2009 when the EU Charter of Fundamental Rights, which contains a right to data protection as well as a right to respect for private life, became legally binding. When the Court annulled an EU law instrument in its entirety for the first time for its incompatibility with the EU Charter, the incompatibility concerned the rights to privacy and data protection .[79] Similarly, the Court first assessed a draft international law agreement for Charter compliance in light of these rights.[80] The Court's caselaw has clearly tended to prioritise privacy and data protection over other competing rights and interests[81] and to conduct strict judicial review of compliance with these rights. This tendency is reflected in the caselaw on data transfers.

The *Schrems I* litigation concerned the refusal of the Irish regulator (the DPC) to investigate a complaint that the EU adequacy mechanism facilitating EU-US data transfers the 'Safe Harbor') was invalid in light of the 2013 Snowden revelations and a prior judgment of the CJEU concerning mass and indiscriminate data processing for law enforcement purposes.[82] This refusal was appealed before the Irish High Court which stayed proceedings to seek clarification from the CJEU concerning the powers and obligations of national regulators when the validity of a European Commission adequacy decision is in doubt. Specifically, the CJEU was asked to consider whether the national supervisory authority (i.e. the DPC or another data protection authority) is

---

[78] Christopher Kuner, 'Article 44. General principle for transfers' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), The EU General Data Protection Regulation (GDPR) - A Commentary (Oxford University Press, 2020), 764-765

[79] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238.

[80] *Opinion 1/15* ECLI:EU:C:2017:592.

[81] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.

[82] *Digital Rights Ireland* (n 79).

bound by the Commission adequacy decision or whether it may or must conduct its own investigations in light of subsequent factual developments.[83] In its judgment, the Court sought to balance the independence of the data protection authorities, guaranteed to ensure their effective monitoring of data protection compliance, with the need to ensure the uniformity of EU law. It concluded that where a national supervisory authority receives a complaint regarding the compatibility of a Commission adequacy decision with fundamental rights, it is incumbent on the national regulator to examine the complaint with all due diligence, however, ultimately only the CJEU can declare an EU act such as an adequacy decision invalid.[84] National law must therefore provide for mechanisms to enable questions of validity to be referred to the CJEU where necessary.[85]

Although not expressly asked to do so, the CJEU went on to examine the validity of the EU-US data transfer mechanism (the Safe Harbor decision) in light of EU law. The Court first provided a definition of adequate protection, as such a definition was not found in the secondary law (Directive 95/46 EC[86], the GDPR's predecessor).

While it recognised that adequate protection signifies that a third country 'cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order', it considered that the protection offered must be 'essentially equivalent' to that offered by EU secondary law read in light of the EU Charter.[87] The CJEU emphasised that it is the legal order of the third country – the applicable rules and the practice designed to ensure compliance with them – that must be adequate and that the Commission must periodically verify this adequacy in law and in practice.[88] Moreover,

---

[83] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650, para 36.
[84] ibid, paras 62 and 63.
[85] ibid, para 65.
[86] Directive 95/46/EC of the European Parliament and of the Coun- cil of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.
[87] *Schrems* (n 83) para 73.
[88] ibid, para 76.

the standard of review conducted by the Commission should be strict, given the number of people concerned and the importance of the rights at stake.[89]

Turning to the specifics of the Safe Harbor decision, the Court considered it to be invalid as, firstly and formalistically, the Commission did not expressly state in that decision that the US 'ensures' an adequate level of protection.[90] Secondly, the Commission had acted ultra vires by including in the decision a provision denying national regulators the powers to investigate complaints relating to data transfers.[91] Although these findings did not require the Court to examine further the substantive content of the safe harbour decision, it nevertheless provided extensive observations on its compatibility with EU law. Notably, it emphasised that the safe harbour principles did not bind public authorities[92] and that national security, public interest and law enforcement requirements under US law have primacy over the safe harbour principles in case of conflict.[93] It observed that US law did not contain any limitations on this interference with fundamental rights or safeguards or effective legal protection against it. These observations set the scene for the subsequent *Schrems II* litigation.

Following the invalidation of the Safe Harbour decision, many EU data exporters (including US technology companies) simply switched from relying on adequacy as a legal basis for data transfers to the use of SCCs as specified in a Commission SCC decision. Following a reformulated complaint from Schrems, the Irish DPC determined in a draft decision that the validity of the Commission's SCC decision was in doubt and commenced litigation before the Irish High Court which culminated in a further reference to the CJEU. In the intervening period following *Schrems I* but before the reference reached the CJEU, the European Commission had adopted a replacement adequacy decision for Safe Harbour entitled Privacy Shield. The Irish High Court referred a series of questions to the CJEU querying, in essence, what role national

[89] ibid, para 78.
[90] ibid, paras 97 and 98.
[91] ibid, paras 102-104.
[92] ibid, para 82.
[93] ibid, para 86.

security considerations should play in determining whether the protection offered by a third country meets the standards of EU law; what role the Commission's SCC Decision plays in determining the legality of data transfers to third countries and whether the Privacy Shield adequacy decision is compatible with EU law.

The CJEU dealt with the national security queries swiftly, finding that when data is transferred between two economic operators for commercial purposes then the transfer is within the scope of the GDPR irrespective of whether the data transferred might subsequently be used for national security purposes in that State.[94] The Court clarified the role of SCCs in the scheme of international data transfers. It observed that the provision on appropriate safeguards falls within Chapter V GDPR and must be read in light of Article 44 GDPR (the General Principles for Transfers). This requires that the level of protection of natural persons guaranteed by the GDPR is not undermined by a transfer. Thus importantly, the Court confirmed that, irrespective of the transfer mechanism used to transfer data to a third country, the same level of protection must be guaranteed.[95] In assessing whether this level of protection is satisfied, SCCs alone are not sufficient. The EU established exporter must also consider relevant aspects of the legal system of the third country. This entails taking account of the factors relevant for adequacy assessments found in Article 45(2) GDPR.[96] The data exporter should conduct this assessment in conjunction with the data recipient in the third country where necessary, an exercise often referred to as a transfer impact assessment.[97] The data exporter is bound to suspend the data transfer where it appears that the recipient cannot comply with the terms of the SCC[98] and, failing this, the national supervisory authority in the EU is required to ensure that the GDPR is fully enforced and shall suspend or prohibit non-compliant data transfers.[99]

---

[94] ibid.
[95] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems II* (*Schrems II*) ECLI**:** EU:C:2020:559, para 92.
[96] ibid, para 104.
[97] ibid, para 134.
[98] ibid, para 140.
[99] ibid, para 112 and 114.

Finally, the scenario before the Irish High Court raised the query about the role of existing adequacy decisions when data exporters and supervisory authorities have doubts about the sufficiency of the protection offered in a third country. The Court reiterated that the supervisory authority remains bound by the adequacy decision until such point as it is invalidated by the CJEU.[100] In examining the compatibility of the Privacy Shield with EU law, the Court noted that the Privacy Shield, like its predecessor, contained a wide-ranging derogation enabling interference with fundamental rights on the basis of national security, public interest requirements or domestic law in the US.[101] While the Commission had considered that such an interference with fundamental rights was limited to what was strictly necessary and that effective legal protection was in place, the Court disagreed.[102] There were two key elements to this. First, the relevant US law indicated no limitations on the power it conferred to implement surveillance programmes for foreign intelligence purposes, which is contrary to the EU law requirement that the legal basis permitting an interference with fundamental rights must itself define the scope of the limitation on the right to comply with proportionality requirements.[103] Secondly, there were aspects of the US legal framework that offered EU residents no possibility to pursue a legal remedy for a violation of their rights. This lacuna – the complete absence of the possibility of legal redress – constitutes an interference with the essence of the right to an effective remedy and, according to the Court, makes it impossible to conclude that the Privacy Shield offered essentially equivalent protection to that offered by EU law.[104] In spite of the redress mechanism of the Privacy Shield Ombudsperson being designed to remedy the lack of legal redress provided by the Safe Harbour system, the Privacy Shield redress mechanism was found to be deficient in important respects. The Ombudsperson was insufficiently independent for the Court, a query was raised about the binding nature of its decisions and the legal safeguards on which individuals could

[100] ibid, para 156.
[101] ibid, para 165.
[102] ibid, paras 167 and 168.
[103] ibid, paras 175, 176, 180.
[104] ibid, paras 187, 191 and 192.

rely.[105] The CJEU concluded that in adopting the Privacy Shield adequacy decision the Commission disregarded the requirements of Article 45(1) GDPR, read in light of Articles 7, 8 and 47 of the EU Charter and it invalidated the decision on that basis with immediate effect.[106] However, it ended the judgment with the observation that the annulment of the Privacy Shield decision would not create a legal vacuum as Article 49 GDPR sets out the conditions in which data transfers to third countries can take place in the absence of an adequacy decision or appropriate safeguards.[107] The implications of this observation, and the *Schrems II* judgment more generally, will be discussed further below.

The CJEU delivered a further finding of significance in the period between the two *Schrems* judgments. It was asked by the European Parliament to opine on, amongst other things, the compatibility with EU law of a draft international agreement concluded between Canada and the EU providing for the sharing of passenger name record (PNR) data by airlines for the purposes of combatting terrorism and serious transnational crime. With the exception of the European Parliament, all other parties to the proceedings (the Member States; the Council and Commission) maintained that the draft agreement was compatible with the provisions of the Treaty on the Functioning of the European Union (TFEU) and the Charter.[108] The Court disagreed. It considered that the failure of the draft agreement to preclude the transfer of sensitive data from the EU to Canada and its subsequent retention and use was incompatible with EU Charter rights.[109] It also set out a list of requirements that the agreement must meet in order for it to be compatible with the EU Charter. This detailed list includes requirements relating to data minimisation and retention; onward data transfers; individual notification rights in specified circumstances; and requirements concerning the level of independence of the relevant supervisory authority, amongst others. This Opinion reveals that the Court is not deferent to the position of the Council or the

[105] ibid, paras 194-196.
[106] ibid, paras 198-199.
[107] ibid, para 202.
[108] ibid, para 51.
[109] Articles 7, 8, 21 and 52(1) EU Charter.

Member States, or the interests of the EU's negotiating partners, when it comes to international arrangements on data transfers. Moreover, just as the *Schrems* jurisprudence sought to reduce the margin of discretion of the European Commission concerning the adoption of adequacy decisions, the detailed guidance stemming from this Opinion reduced the margin for manoeuvre of the EU Council when seeking to renegotiate an EU-Canada PNR agreement.

The case law of the CJEU concerning data transfers is consequently very significant to the question of continuing UK adequacy. The CJEU has demonstrated a willingness to invalidate acts of the Commission, international agreements and EU legislative instruments more broadly when the relevant instruments do not conform to EU fundamental rights standards. Adequacy and other mitigation measures are assessed strictly, and the assessment is shaped by fundamental rights concerns. The trade orientation and pragmatism of the Commission is contrasted with the CJEU's emphasis on rights and the championing of the rights to respect for private life and protection of personal data.

3.3 Adequacy in Practice

To date, 19 adequacy decisions have been adopted by the Commission and analysed for this report. Under the Data Protection Directive, adequacy decisions were adopted for Andorra, Argentina, Canada, Faro, Guernsey, Hungary (before it joined the EU), the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay, all of which remain in force pursuant to Article 45(9), GDPR.[110] Since the GDPR has been

[110] Commission Decision 2010/625/EU on the adequate protection of personal data in Andorra.[2010] OJ L 277/27; Commission Decision 2003/490/EC on the adequate protection of personal data in Argentina. [2003] OJ L 168/19; Commission Decision 2002/2/EC on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. [2001] OJ L 2/13; Commission Decision 2010/146/EC on the adequate protection provided by the Faeroese Act on processing of personal data. [2010] OJ L 58/17; Commission Decision 2003/821/EC on the adequate protection of personal data in Guernsey. [2003] OJ L 308/27; Commission Decision 2000/519/EC on the adequate protection of personal data provided in Hungary. [2000] OJ L 215/4; Commission Decision 2004/411/EC on the adequate protection of personal data in the Isle of Man.

adopted, the Commission has adopted adequacy decisions recognising as adequate Japan,[111] Korea[112] and the United Kingdom (under both the GDPR[113] and the Law Enforcement Directive[114]). Additionally, three adequacy decisions have been adopted regarding transfers to the United States: Safe Harbor[115] and Privacy Shield[116] under the Data Protection Directive, which were invalidated in *Schrems I* and *Schrems II* respectively, and the EU-US Data Privacy Framework[117] adopted recently on 10 July 2023 under the GDPR. More limited forms of adequacy decision are also sometimes adopted which can be relevant to data transfers, including limited arrangements regarding the transfer of Passenger Name Records associated with international travel, and the transfer of certain auditing and accounting information under Directive 2006/43/EC. These other types of limited adequacy decisions have not been considered in compiling this report as they are not suitable to address general commercial and public sector data transfers.

[2004] OJ L 151/48; Commission Decision 2011/61/EU on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. [2011] OJ L 27/39; Commission Decision 2008/393/EC on the adequate protection of personal data in Jersey. [2008] OJ L 138/21; Commission Decision 2013/65/EU on the adequate protection of personal data by New Zealand. [2012] OJ L 28/12; Commission Decision 2000/518/EC on the adequate protection of personal data provided in Switzerland. [2000] OJ L 215/1; Commission Implementing Decision 2012/484/EU on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data. [2012] OJ L 227/11.

[111] Commission Implementing Decision 2019/219/EU on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. [2019] OJ L 76/1.

[112] Commission Implementing Decision 2022/254/EU on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act. [2021] OJ L 44/1.

[113] Commission Implementing Decision 2021/1772/ EU on the adequate protection of personal data by the United Kingdom. [2021] OJ L 360/1.

[114] Commission Implementing Decision 2021/1773/EU on the adequate protection of personal data by the United Kingdom. [2021] OJ L 360/69.

[115] Commission Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. [2000] OJ L 215/7.

[116] Commission Implementing Decision 2016/125/EU on the adequacy of the protection provided by the EU-U.S. Privacy Shield. [2016] OJ L 207/1.

[117] Commission Implementing Decision 2023/4745/EU on the adequate level of protection of personal data under the EU-US Data Privacy Framework. [2023] [Not yet published in the Official journal, available at https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf]

What emerges from this analysis is that the Commission has, as it claims, recognised 'a diverse range of privacy systems, representing different legal traditions, as being adequate'.[118] It is also apparent that a clear divergence exists between the adequacy assessments conducted prior to and following the *Schrems* jurisprudence and the adoption of the GDPR. The Commission's interpretation of adequacy has become stricter and more detailed over time.[119] Nevertheless, despite a more rigorous approach to adequacy assessments over time, the Commission appears inclined to adopt adequacy findings, sometimes recognising exceptions to their scope, resulting in decisions with very different scopes of application. A further relevant finding is that the dominant focus of the Commission's analysis is on "law on the books" rather than the reality of its interpretation and enforcement on the ground.

The implications of this body of adequacy decisions for the Commission's reappraisal of the UK's adequacy will be considered in Section 4.6. This section will briefly outline (i) the process of adopting adequacy decisions; (ii) the typical structure of an adequacy decision; (iii) the scope of adequacy decisions; and (iv) the relevant factors for a finding of adequacy.

(i) The process of adoption

The EU Commission is empowered to adopt adequacy decisions pursuant to Article 45(1) GDPR.[120] The European Data Protection Board (EDPB), and before it, the Article 29 Working Party (A29WP), has an important role in the assessment of adequacy. For every decision that is adopted, the EDPB or A29WP have provided an opinion on adequacy. This role was formalised in the GDPR.[121] In addition, the EDPB

[118] David Erdos, 'The UK and the EU personal data framework after Brexit: A new trade and cooperation partnership grounded in Council of Europe Convention 108+?' (2022) Computer Law and Security Review 1, 2.

[119] As Erdos observes, the 'EU's interpretation of adequacy remains shrouded in considerable uncertainty but has clearly become stricter over time'. ibid.

[120] Previously under Article 25(6) Directive 95/46 (n 86).

[121] Article 70(1)(s) GDPR.

has had an important influence over adequacy by establishing the criteria used to determine whether a third country is adequate in two important opinions which, as discussed below, have shaped the analysis conducted.

The process by which the Commission initiates adequacy decisions is not entirely transparent. The European Parliament had recommended greater transparency over the rules of conducting adequacy assessment, including initiation, and the ongoing assessment of adequacy assessments during the GDPR reform process.[122] Despite these recommendations 'the "logistics" of how adequacy decisions are to be issued and used' was not defined very explicitly.[123] However, alongside the clarifications introduced in the GDPR, in 2017 the Commission issued a communication which explains its approach to data transfers, including adequacy.[124] In this communication, the Commission argues that 'it is possible for the Commission to recognise a diverse range of privacy systems, representing different legal traditions, as being adequate.'[125] The Commission identifies four criteria which should be considered when determining whether a dialogue on adequacy should be pursued:

(i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;

(ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;

(iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and

[122] European Parliament, 'Reforming the Data Protection Package' (21 September 2012), 70. <https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET(2012)492431_EN.pdf>.

[123] ibid.

[124] Communication from the Commission to the European Parliament and the Council, 'Exchanging and Protecting Personal Data in a Globalised World' COM [2017] 7 final.

[125] ibid, 7.

(iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[126]

These factors would suggest that the UK is a desirable candidate for an adequacy decision, provided the political relationship between the UK and the EU remains constructive

Existing adequacy decisions are inconsistent in terms of disclosure of details of the initiation stages. However, in at least a few of the associated opinions of the A29WP, the nature of the request from the third country is mentioned. For Andorra, Argentina, Israel and Uruguay the request came from the relevant ambassador/mission to the EU.[127] In the latest EU-US Data Privacy Framework, the decision explicitly states that '[f]ollowing the Schrems II judgment, the Commission entered into talks with the U.S. government with a view to a possible new adequacy decision that would meet the requirements of Article 45(2) of Regulation (EU) 2016/679 as interpreted by the Court of Justice.'[128]

The assessment is often dynamic, with multiple exchanges of information between the parties. In the Data Protection Directive era, the A29WP seems to have engaged directly with the state in question via their data protection authority,[129] while in the GDPR era, the Commission seems to have taken over this role, and instead provides information gathered to the EDPB for them to provide their opinion.[130]

Notably, at least a few of the adequacy decisions seem to be reached through law reform on foot of these negotiations. For example, the A29WP explicitly encouraged the Andorran authorities to adopt new legislation to address automated decision

[126] ibid, 8.
[127] See A29WP- Opinion 7/2009; Opinion 4/2002; Opinion 6/2009; Opinion 6/2010.
[128] Commission Implementing Decision 2023/4745/EU, Recital 6.
[129] Seen for example in the case of the Faroe Islands (Opinion 9/2007); Hungary (Opinion 96/99); Israel (Opinion 6/2009); New Zealand (Opinion 11/2011); Uruguay (Opinion 6/2010).
[130] See statements in Japan (Opinion 28/2018); Korea (Opinion 32/2021); UK (Opinion 14/2021); US (Opinion 5/2023).

making,[131] and similarly recommended law reform to the Israeli authorities.[132] As part of the EU/Korean discussions, a Korean 'Notification' (a type of delegated legislative instrument) was adopted which clarified the interpretation and application of Korean data protection legislation which was necessary in order to find adequacy.[133] In order to conclude the Japanese adequacy decision, a set of Supplementary Rules for data transferred from the EU was agreed and adopted in Japanese law (also appended to the decision).[134] The EU-US Data Privacy Framework makes reference to the EU-US discussions which led to the US adopting 'Executive Order 14086 "Enhancing Safeguards for US Signals Intelligence Activities" (EO 14086), which is complemented by a Regulation on the Data Protection Review Court issued by the U.S. Attorney General (AG Regulation).'[135]

Further, many of the adequacy decisions are contingent on some assurances by the third country on their legal system or practices, deriving in some cases from the national data protection authority and in other cases from governmental authorities. The Andorran,[136] Argentinian,[137] and Israeli[138] decisions make mention of such

[131] Commission Decision 2010/625/EU, recital 14.
[132] Commission Decision 2011/61/EU, recital 15.
[133] Commission Implementing Decision 2022/254/EU, Annex I.
[134] Commission Implementing Decision 2019/219/EU, Annex I.
[135] Commission Implementing Decision 2016/125/EU, recital 6.
[136] Commission Decision 2010/625/EU, recital 11 provides: 'Andorran data protection authorities have provided explanations and assurances as to how the Andorran law is to be interpreted, and has given assurances that the Andorran data protection legislation is implemented in accordance with such interpretation. This Decision takes account of those explanations and assurances, and is therefore conditional upon them.'
[137] Commission Decision 2003/490/EC, recital 15 provides: 'The Argentine government has provided explanations and assurances as to how the Argentine law is to be interpreted, and has given assurances that the Argentine data protection rules are implemented in accordance with such interpretation. This Decision is based on these explanations and assurances, and is therefore conditional upon them. In particular, this decision relies on the explanations and assurances given by the Argentine authorities as to how the Argentine law is to be interpreted as regards which situations fall within the scope of the Argentine law in data protection.'
[138] Commission Decision 2011/61/EU, recital 11 provides: 'Israeli data protection authorities have provided explanations and assurances as to how the Israeli law is to be interpreted, and have given assurances that the Israeli data protection legislation is implemented in accordance with such interpretation. This Decision takes account of these explanations and assurances, and is therefore conditional upon them.'

assurances. In a step further, in the GDPR era, those assurances are explicitly annexed to some of the decisions themselves, in the case of Japan[139] and Korea.[140] The Privacy Shield and EU-US Privacy Framework decisions contains a series of annexed letters which are not expressly labelled assurances but are functionally so.[141] Neither of the UK adequacy decisions refer to any such assurances or append any supporting materials.

(ii) The typical structure of an adequacy decision

There have been two major changes to adequacy decisions over time. First, the GDPR era adequacy decisions are considerably longer, and contain lengthy findings by the Commission on the legal system being assessed which support its determination of adequacy. Second, after *Schrems I,* all the pre-existing adequacy decisions were amended to (i) broaden the competence of the EU national supervisory authorities to oversee data transfers subject to adequacy decisions, and (ii) introduce an ongoing monitoring obligation upon the Commission, such that adequacy decisions must be subject to review reports.[142] The UK adequacy decisions are the only decisions (discussed below) which contain a sunset clause and will end unless subject to a positive subject review by the Commission. Only one review report has been released to date, regarding Japan, which reports favourably on increased convergence between EU and Japanese systems.[143]

All adequacy decisions have a similar layout. First, we find the recitals (which are non-binding, but guide the interpretation of the instrument). The recitals generally contain (a) an overview of what an adequacy decision is and the relevant provisions of the GDPR/Data Protection Directive, (b) a description of the third country, and the relevant

[139] Commission Implementing Decision 2019/419/EU, Recital 4, Article 1(1), Annex II.
[140] Commission Implementing Decision 2022/254/EU. Recital 6, Article 1(1), Annex II.
[141] See Commission Decision 2013/65/EU, Annex III-VII; Commission Implementing Decision 2023/4745/EU, Annex II-VII.
[142] Commission Implementing Decision (EU) 2016/2295.
[143] European Commission Report, on the first review of the functioning of the adequacy decision for Japan, [2023] COM 275 final.

laws affecting data protection, and (c) a statement of the opinion of adequacy. In the early decisions element (b) is very short, comprising a few paragraphs, whereas now these descriptions run between 20-75 pages, excluding supporting annexes, illustrating the increased detail regarding the findings that are now included within the decision itself. Second, the operative articles of the decision contain several elements. Article 1 typically contains the statement of adequacy and any exclusions as to the scope of the adequacy decision. The remainder of the articles tend to address the continuing power of DPAs to monitor data flows, the requirement of the Commission to monitor the application of the third country to assess whether adequacy continues, and information sharing and reporting requirements.

(iii) The scope of the adequacy decision

One important area of divergence between adequacy decisions concerns the scope of the finding of adequacy decision. Several decisions are findings of partial adequacy. Two early examples of narrower scope of adequacy are Canada and Israel.[144] For instance, the Canadian decision applies only to recipients who are subject to the Canadian data protection legislation (Personal Information Protection and Electronic Documents Act).[145]

Narrower decisions are more common in the GDPR era, as all the adequacy decisions adopted post 2016 have at least some exclusions regarding scope. The Korean adequacy decision excludes processing of personal data for missionary activities by religious organisations and for the nomination of candidates by political parties, or the processing of personal credit information pursuant to the Korean Credit Information

[144] The Israeli decision applies on to data subject to automated processing and not manual data. Commission Decision 2011/61/EU, Article 1(1) provides: "For the purposes of Article 25(2) of Directive 95/46/EC, the State of Israel is considered as providing an adequate level of protection for personal data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel."

[145] Commission Decision 2002/2/EC, Article 1 provides: "For the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act ('the Canadian Act')."

Act by controllers that are subject to oversight by the Financial Services Commission.[146] The Japanese adequacy decision applies only to commercial operators and excludes data provided to recipients in the following categories: (a) broadcasting and press organisations, (b) professional writers, (c) universities and academic groups and organisations, (d) religious bodies and (e) political bodies.[147] The EU-US Data Privacy Framework facilitates data transfers only to organisations which self-regulate according to the Data Privacy Framework approach.[148] The UK GDPR adequacy decision excludes immigration control data.[149]

Arguably, some of the earlier adequacy assessments accept statements of practice or legal positions which seem equivalent to those which have required exclusions from adequacy decisions in the GDPR era. We might contend that this is representative of the tightening of the assessment post-*Schrems*. For example, in the Jersey A29WP opinion there is some concern around the definition of manual data, but the Party finds 'the extent to which these types of less structured manual files are likely to be transferred from an EU member state to Jersey is small. This situation does not therefore pose a serious obstacle to consider the Jersey Law as providing adequate protection in respect of its handling of manual record systems.'[150]

(iv) The factors relevant to assessing adequacy

Article 45(2) of the GDPR specifically provides factors that the Commission must take account of when assessing adequacy, particularly: (a) the rule of law, human rights and fundamental rights standards, relevant legislation (including public authority access to data), and rules concerning onward transfers, data subject rights and effective judicial and administrative redress; (b) the existence and effective functioning

[146] Commission Implementing Decision 2022/254/EU, Recital 4, Article 1(2).
[147] Commission Implementing Decision 2019/219/EU, Recitals 37-38, Article 1.
[148] Commission Implementing Decision 2023/4745/EU, Article 1.
[149] Commission Implementing Decision 2021/1772/ EU, Recital 6, Article 1(2).
[150] Opinion 8/2007, 6.

of one or more independent supervisory authorities and (c) international commitments to which that third country is subject.

In general, the assessments are formal reviews of the national law "on the books" concerning data processing, any relevant rights protections (including international treaties), and laws which provide for law enforcement or national security access to data. There is minimal consideration of enforcement, though short summaries of recent enforcement activities by relevant national supervisors is mentioned in a number of the GDPR era decisions[151] and in the UK GDPR decision reference is made of actions brought against the UK before the European Court of Human Rights.[152] In the first Japanese review report, it is noted that there had been no enforcement activity over the supplementary rules adopted under that adequacy decision for the two years since it adopted.[153]

A review of the adequacy decisions adopted to date demonstrates that the majority closely follow the process for review set out by the A29WP, then the EDPB. Those adopted under the Data Protection Directive largely assess the laws of the third country by reference to a Working Document adopted by the A29WP in 1998, 'Transfers of

---

[151] Korea, Recital 128; Commission Implementing Decision 2021/1772/ EU, Recital 95-97. Regarding Japan, a very brief mention is made of use of enforcement powers against Facebook, Commission Implementing Decision 2019/219/EU, Recital 97. US, Recitals 62-63, Commission Implementing Decision 2023/4745/EU, mentions enforcement action regarding Privacy Shield (around 22 cases) and general enforcement activity regarding data protection requirements.

[152] Commission Implementing Decision 2021/1772/ EU (n 113), Recital 111.

[153] Report from the Commission on the first review of the functioning of the adequacy decision for Japan. 3 April 2023 COM(2023) 275 final (p 5) provides: 'As regards oversight and enforcement, the Commission notes that the PPC has made more use of its non-coercive powers of guidance and advise (Article 147 APPI) than of its coercive powers (e.g. to impose binding orders, Article 148 APPI) in the period following the adoption of the adequacy decision. The PPC also reported that to date, no complaints concerning compliance with the Supplementary Rules have been received, and no investigations into such issues have been conducted on the PPC's own initiative. During the review meeting, however, the PPC announced that it is considering conducting, on its own initiative, random checks to ensure compliance with the Supplementary Rules. The Commission welcomes this announcement, as it considers that such random checks would be very important to ensure that (possible) violations of the Supplementary Rules are prevented, detected and addressed, thereby ensuring effective compliance with these rules. As the 2020 and 2021 amendments of the APPI have strengthened the PPC's oversight powers, these random checks could be part of an overall effort to increase the use of such powers.'

personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP12).[154] After the adoption of the GDPR, an updated version of this advice was prepared (WP254),[155] which represents an extension of the original list, rather than any wholesale rewrite. WP254 was also revised after *Schrems I*. Additionally, adequacy decisions adopted in the GDPR era which assess public authority/law enforcement access to data are guided by an additional guidance document adopted by the Article 29 Working Party (WP237).[156]

WP254, and previously WP12, are said to represent the 'core data protection principles' or minimum standards which must be in place in order for an adequacy assessment to be successful.[157] The data protection laws of the third country are assessed by reference to essential 'content principles', 'procedural and enforcement mechanisms' and 'essential guarantees for law enforcement and national security access to limit interferences to fundamental rights'. With regard to the 'content principles', the elements to be assessed may be summarised as follows[158]:

- basic equivalent data protection concepts, including 'personal data', 'processing', 'data controller', 'data processor', 'recipient' and 'sensitive data';
- grounds for lawful and fair processing for legitimate purposes, set out in a sufficiently clear manner,
- the purpose limitation principle;
- the data quality and proportionality principle;
- the data retention principle;
- the security and confidentiality principle;
- the transparency principle;

---

[154] A29WP, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', adopted on 24 July 1998, WP 12.
[155] A29WP, 'WP254' (n 4).
[156] A29WP, 'Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)', adopted on 13 April 2016, WP 237.
[157] A29WP, 'WP12' (n 154) 5; A29WP, 'WP254' (n 4) 3.
[158] Elements which were added in WP254 in the GDPR era and which were not reflected in the earlier WP12 are underlined.

- rights of access, rectification, erasure and objection;
- restrictions on onwards transfers of data.

Additional content principles must be in place with regard to specific types of processing, in particular:

- Additional safeguards for special categories of data;
- An ability to object to direct marketing; and
- Safeguards regarding automated decision making and profiling.

The third country must also offer adequate procedural and enforcement mechanisms, in particular:

- The existence of a competent independent supervisory authority, which must 'act with complete independence and impartiality', and have necessary powers and responsibilities;[159]
- The data protection system must ensure a good level of compliance. This is described as ensuring accountability and awareness amongst controllers and processors, and subject awareness, and noting sanctions and supervision have an important role in ensuring respect for the rules.[160]
- Accountability (Controllers must be obliged to comply with the law and demonstrate such compliance.)[161]
- The availability and support of individual remedies and redress mechanisms, so individuals can enforce their rights 'rapidly and effectively, and without prohibitive cost'.[162]

In the GDPR era, the adequacy decisions themselves contain findings according to the WP254 criteria, and while the EDPB opinions associated with these third countries continue to follow these criteria, notably it tends to place greater focus on the areas of concern at the outset of its Opinions, where there are either gaps in terms of protection or where the EDPB wants to encourage the Commission to require further

[159] A29WP, 'WP254' (n 4) 7.
[160] ibid.
[161] ibid, 8.
[162] ibid.

information.[163] For example, regarding the UK GDPR adequacy assessment, the EDPB points to the need for further attention to the immigration exemption and onward transfers in particular.[164]

3.4 UK Adequacy Decisions

The Trade and Cooperation Agreement (TCA)[165], which entered into force on 1 May 2021, provides for the terms of future trading between the UK and the EU. The TCA contains a title on Digital Trade which includes a chapter on data flows and data protection. The general provisions chapter includes a broad 'right to regulate' of the respective parties, reaffirming 'the right to regulate within their territories to achieve legitimate policy objectives' including privacy and data protection.[166] Importantly, Article 202(1) TCA confirms that both parties recognise that individuals have a right to the protection of personal data and privacy. However, it brings personal data regulation outside of the scope of the TCA to a large extent.[167] Article 202(2) provides:

> Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred.

Therefore, subject to the proviso that whatever data protection and privacy measures adopted are formulated in objective terms and apply horizontally[168], both the EU and

---

[163] See Opinion 28/2018 (Japan); Opinion 32/2021 (Korea).
[164] EDPB, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom' adopted on 13 April 2021.
[165] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ire- land, of the Other Part, [2021] OJ L149/10.
[166] Article 198 TCA.
[167] Article 525 TCA governs data sharing for passenger name records (PNR),criminal records and also DNA, fingerprint and vehicle registration data.
[168] The definition of 'conditions of general application' is found in footnote 1 to Article 202 TCA.

the UK can maintain their own data rules on cross-border data transfers. This is in keeping with the EU's broader policy of maintaining a separation between the negotiation and conclusion of trade agreements and the conduct of data protection adequacy assessments. To avoid a legal vacuum between the end of the transition period (31 December 2020) and the conclusion of the Commission's adequacy assessment, a bridging period was agreed between the UK and the EU.[169] The Commission adopted two adequacy decisions recognising the adequacy of the UK for GDPR[170] and Law Enforcement Directive purposes respectively on 28 June 2021.[171] The focus of this report is on the former.

In keeping with the post-GDPR evolution in adequacy decisions noted above, the decision is detailed and lengthy. It notes that the standards against which adequacy, or essential equivalence, are assessed are those found in the GDPR and the jurisprudence of the CJEU with the significance of the EDPB's adequacy referential also noted.[172] It emphasises that adequacy does not entail a 'point-to-point replication of Union rules' but rather considers whether the system as a whole in a third country delivers adequate protection.[173]

The UK data protection framework consists of the DPA 2018, through which the UK availed of the flexibilities afforded by the GDPR and adopted specific provisions on law enforcement[174] and national security[175], and the UK GDPR, which mirrors the EU GDPR. Both were subject to modifications by secondary legislation (the DPPEC Regulations). These modifications were primarily of a technical nature (for instance, to replace references to the EU with the UK or to reflect the purely domestic nature of the rules). The Commission concluded that in both its structure and main components, the

[169] Article 782 TCA.
[170] Commission Implementing Decision 2021/1772/ EU (n 113) recital 5.
[171] The LED Adequacy was the first of its kind. Erdos, 'The UK and the EU personal data framework after Brexit' (n 118) 2.
[172] Commission Implementing Decision 2021/1772/ EU (n 113) recital 3.
[173] ibid recital 4.
[174] UK Data Protection Act (DPA) 2018, part 3.
[175] UK Data Protection Act (DPA) 2018, part 4.

UK legal framework is very similar to that of the EU. It emphasised that the legal framework has been shaped by EU law and adherence to legally binding international instruments.[176] The Commission then structured its analysis around two key areas. First, a consideration of the key rules applicable to personal data processing. This included an assessment of elements such as the scope of the rules, the definition of core concepts, the safeguards, rights and obligations provided by the framework and the provisions on oversight and enforcement. The decision highlights that, given their relevance for the effective exercise of individual rights, any relevant developments regarding the interpretation and application in practice of exemptions to these rights such as those for journalism or immigration will be considered in monitoring.[177] The second major area for analysis concerns access and use of personal data transferred from the EU to the UK by public authorities in the UK. In this part, the Commission conducts an analysis of the legal regimes for data access and use for law enforcement and national security purposes respectively. The Commission concludes that any interferences with fundamental rights for these public interest purposes are limited to what is strictly necessary to achieve these interests and that effective legal protection against these interferences exist.[178] The Commission also considered that the oversight and redress mechanisms available to enable infringements to be identified and sanctioned in practice as well as the legal remedies available to individuals were adequate.[179] The availability of appropriate redress under the Human Rights Act and before the European Court of Human Rights were of significance here.[180] Indeed, it is evident throughout the adequacy decision that the Commission's assessment placed significance emphasis on the UK's ratification of Convention 108 as well as its Council

[176] Commission Implementing Decision 2021/1772/ EU (n 113) recital 19.
[177] ibid, recital 73.
[178] ibid, recital 275.
[179] ibid, recital 274.
[180] ibid recital 19 and recitals 109-111.

of Europe membership, its adherence to the ECHR and its submission to the jurisdiction of the European Court of Human Rights.[181]

The adequacy decision excluded from its scope personal data falling within the scope of the immigration exemption found in UK law.[182] This exemption avails of the possibility afforded by Article 23 GDPR to prevent data subjects from exercising certain data protection rights when necessary for particular purposes, in this instance that of effective immigration control. The UK Court of Appeal had held that the UK's implementation of this exemption lacked specific provisions setting out the safeguards provided for by Article 23(2) GDPR.[183] The Commission excluded transfers of data to which the immigration exception could be applied from the scope of the decision.[184] The Commission assumes through this exclusion that the data once transferred can be ring-fenced and will not be made available for immigration control purposes. The EDPB implicitly queries this assumption in its Opinion, highlighting that the exemption also applies where personal data are made available by the controller to another controller who then subsequently processes this personal data for immigration purposes.[185] Moreover, the Commission suggests that transfers for immigration purposes might nevertheless be carried out even in light of this finding of inadequacy on the basis of the other mechanisms found in Articles 46-49 GDPR provided that 'the applicable conditions are fulfilled'.[186] While this suggestion finds support in Article 45(7) GDPR, which specifically states that a Commission decision repealing, amending or suspending adequacy decisions to the extent necessary is without prejudice to transfers pursuant to Articles 46-49, any transfer would nevertheless need to comply with the requirements stemming from the Court's *Schrems II* jurisprudence.

---

[181] ibid recital 119 and 120 and recital 277. In recital 19 it states that adherence to the ECHR, Convention 108 and submission to the jurisdiction of the ECtHR are a 'particularly important element of the legal framework assessed in this Decision'.

[182] UK Data Protection Act 2018, Schedule 2, para 4(1).

[183] *R (Open Rights Group and the3million) v Secretary of State for the Home Department and Others* [2021] EWCA Civ 800.

[184] Commission Implementing Decision 2021/1772/ EU (n 113) recital 6.

[185] EDPB, 'Opinion 14/2021' (n 164) para 12.

[186] ibid, footnote 9.

From one perspective, the finding that the UK offered an adequate level of protection in the immediate aftermath of its exit from the EU is unsurprising. It would have been difficult for the Commission to suggest that its status changed from adequate to inadequate from one day to the next. Nevertheless, the CJEU had previously declared the UK's data retention regime for telecommunications metadata to be incompatible with the EU Charter.[187] On this basis, it was reasonable to query whether the legal regime for data access and use for law enforcement and national security purposes would meet the strict requirements of the Court's jurisprudence.[188] In its Opinion on the draft decision, the EDPB identified several 'challenges' concerning the compatibility of the legal regime for data access and use for these purposes with existing EU law. However, ultimately the EDPB simply invited the Commission to address these challenges in its decision, an invitation which the Commission did not take up.

The Commission did however commit to monitoring developments in the UK closely, in line with the EDPB's recommendation[189], noting that such monitoring is particularly important given that once the UK is no longer bound by EU law it will 'administer, apply and enforce a new data protection regime…which may be liable to evolve'.[190] The Commission indicated the factors that it would pay special attention to in conducting this monitoring.[191] The possibility of a change of legislative framework in the UK also motivated the Commission to include a sunset clause in the adequacy decision which will apply four years following its entry into force. The process for review of the adequacy decision should be initiated by the Commission at least six months before the Decision ceases to apply (i.e. by December 2024 at latest). Any legislative change introduced by the DPDI (No 2) Bill is therefore likely to be an integral part of this revised

[187] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970.
[188] Andrew Murray, 'Data transfers between the EU and UK post Brexit?' (2017) 7 International Data Privacy Law 149, 153.
[189] EDPB, 'Opinion 14/2021' (n 164) para 37.
[190] Commission Implementing Decision 2021/1772/ EU (n 113) recital 281.
[191] ibid.

adequacy assessment, with the Commission paying particular attention to the issues it considered relevant to its ongoing monitoring.

4 Proposed Legal Changes: The Data Protection and Digital Information (No 2) Bill

4.1 The Future Direction of UK Digital Policy

In a preparatory effort to exercise post-Brexit regulatory freedom and align with the National Data Strategy, the Department for Digital, Culture, Media & Sport (DCMS) launched a public consultation for the reform of UK data protection law.[192] The consultation document, 'Data: A New Direction' was published in September 2021 with a stated intention of creating an 'ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data.'[193] The economic value of data as a 'strategic asset' is at the forefront of the document which holds that the reshaping of the data protection regime has the potential to 'drive growth, innovation and competition across the country.'[194] Shortly after the publication of the Government response to the consultation,[195] the Data Protection and Digital Information Bill was introduced in the House of Commons with the promise to 'seize the benefits of Brexit and transform the UK's independent data laws.'[196]

---

[192] 'National Data Strategy' (GOV.UK) <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy> .

[193] Department for Digital, Culture, Media & Sport (DCMS), 'Data: A New Direction' (2021).

[194] ibid.

[195] Department for DCMS, 'Data: A New Direction - Government Response to Consultation', 23 June 2022. <https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation> .

[196] 'Matt Warman (The Minister of State, DCMS) Data Protection and Digital Information Volume 718: Debated on Monday 18 July 2022 [HCWS210]' <https://hansard.parliament.uk/commons/2022-07-18/debates/22071813000008/DataProtectionAndDigitalInformation>.

The Data Protection and Digital Information (No 2) Bill, which supersedes the original Data Protection and Digital Information Bill,[197] was introduced in the House of Commons on 8 March 2023. The DPDI (No 2) Bill has reached report stage in the House of Commons, having been amended at Committee Stage.[198] It has been noted that much of the content of the revised Bill is the same as the original.[199] The Secretary of State for the Department for Science, Innovation and Technology, Michelle Donelan, highlighted that a co-design process with stakeholders led to several changes in the second iteration of the Bill including changes regarding the reduction of compliance costs, paperwork, increasing confidence in AI technologies.[200] According to the Minister, the Bill creates 'a new UK data rights regime tailor-made for our needs'.[201] In her written statement accompanying the Bill, she positioned the Bill as an important part of a clear mission to ensure that the UK is the 'most innovative economy in the world'. According to the written statement:

> Better data access and use is at the heart of our mission to grow the economy, to improve the lives of everyone in the UK, and to achieve the Prime Minister's five key priorities. Data is fundamental to economic growth, scientific research, innovation, and increasing productivity.[202]

The Written Statement emphasised the economic benefits of the Bill, stating that it is designed to reduce the burden on business and should boost the UK economy by £4.7 billion over the next decade.[203] Importantly, the Written Statement also recognised the

---

[197] The original Data Protection and Digital Information Bill was introduced to the House of Commons in July 2022 and was withdrawn by the Government when the Data Protection and Digital Information (No 2) Bill was introduced.

[198] Data Protection and Digital Information (No 2) Bill (As amended in Public Bill Committee).

[199] John Woodhouse, 'The Data Protection and Digital Information (No 2) Bill: Commons Stages' <https://commonslibrary.parliament.uk/research-briefings/cbp-9803/>.

[200] HC Deb 8 March 2023, vol 729, cols 19-22WS.

[201] ibid.

[202] ibid.

[203] ibid. The Impact Assessment for the Bill estimated that Net Present Value for the UK of the Bill to be between £1.2 billion and £9.1 billion with a central estimate of £4.7 billion over ten years. 'Impact Assessment: Data Protection and Digital Information (No.2) Bill' [2023]

importance of data protection principles in enabling free trade with global partners, noting that 81% of trade in services is enabled by international data flow. In addition to stating the Government's intention to make new international data transfer agreements, the need to engage with the EU and its institutions was also acknowledged as was the importance of ensuring that the EU's UK data decisions remain in place.[204]

In the following sections we will identify the key changes proposed in the DPDI (No 2) Bill that may impact on the future adequacy status of the UK.

4.2 Independence and Political Influence

The EDPB's WP254 document highlights the importance for adequacy of the existence of a competent independent supervisory authority, which must 'act with complete independence and impartiality', and have necessary powers and responsibilities.[205] This section identifies the potential impact that the DPDI (No 2) Bill will have on the independence and effectiveness of the Information Commissioner's Office (the ICO), the UK's supervisory authority.

According to the Secretary of State, the DPDI (No 2) Bill will transform the Information Commissioner's Office (ICO) 'to ensure it is ready to tackle new challenges and protect citizens from the most serious harms, while supporting innovative use of data'.[206]

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1151358/data_protection_and_digital_information_bill_impact_assessment_march_2023.pdf>.
It should be noted that the Impact Assessment has been criticised, including on the grounds that the Impact Assessment does not factor in the costs that would face UK companies trading into Europe who would be obliged to comply with the GDPR and the new UK regime. Amberhawk, 'New DPDI Bill Savings Inflated by 324%; Loss of Adequacy Agreement Would Cost UK over £2 Billion' (Hawktalk, 28 March 2023) <https://amberhawk.typepad.com/amberhawk/2023/03/new-dpdi-bill-savings-inflated-by-324-loss-of-adequacy-costs-uk-over-2-billion.html>.

[204] HC Deb 8 March 2023 (n 200).

[205] A29WP, 'WP254' (n 4) 7.

[206] HC Deb 8 March 2023 (n 200).

At present, the ICO is established as a Corporation Sole with all formal powers and duties resting with the Commissioner.[207] Nevertheless, due to the 'scale and complexity of the ICO's role and remit, and in line with good practice', the Information Commissioner has instituted a Management Board comprised of Executive and Non-Executive Directors.[208] The Commissioner chairs the Management Board and is responsible for 'setting the strategic direction' for the ICO.[209] The Commissioner retains the right to 'set a course of action that is contrary to the majority view of the Board', but will set out the reasoning behind such a decision in their Annual Report.[210]

Under the DPDI (No 2) Bill, the ICO will be abolished and replaced with a new Information Commission which would be established as a body corporate in line with other UK regulators.[211] Schedule 13 of the DPDI (No 2) Bill[212] begins by noting that the Commission is not to be regarded 'as a servant or agent of the Crown'. The Commission will comprise non-executive members appointed by the Secretary of State and executive members including a chief executive appointed by the non-executive members and such other members, if any, as the non-executive members may appoint.[213] Schedule 13 requires the non-executive members to consult the Secretary of State before appointing

---

[207] ICO, Decision making structure https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/.

[208] ibid.

[209] ibid. As detailed on the ICO website: 'The Commissioner has designated that the Management Board will operate on a collective decision-making model, and the same model is used for the various Committees and Boards which support the Management Board. The Board operates on a 'majority vote' principle in circumstances where a consensus view cannot be reached. The Commissioner, as a Corporation Sole, will always have the right to set a course of action that is contrary to the majority view of the Board. In such circumstances, the Commissioner will publish the rationale for their decision as part of the Commissioner's Annual Governance Statements in the Annual Report and Accounts to Parliament. In terms of the Executive leadership of the ICO, the Commissioner has formally delegated the responsibility for the regulatory functions, administrative leadership and performance of the organisation through the Executive Team.'

[210] ibid.

[211] DPDI (No 2) Bill (n 198) 107-108. DCMS, 'Data: A New Direction – government response' (n 195).

[212] Intended to be inserted as Schedule 12A to the Data Protection Act 2018.

[213] The number of members will be between three and 14 and this will be determined by the Secretary of State The non-executive members will include 'a chair appointed by His Majesty by Letters Patent on the recommendation of the Secretary of State' and 'such other members as the Secretary of State may appoint.'

the CEO. Notably, in the initial call for consultation documents, the Government had proposed appointing the CEO via the public appointment process. This proposal was criticised by, amongst others, the current Information Commissioner, John Edwards, on the grounds that it would have hindered the ICO's independence. Following this criticism, the procedure was adjusted to allow for the CEO's appointment by the board in consultation with the Secretary of State.[214]

Edwards has since expressed support for the modified proposals in the DPDI (No 2) Bill. In fact, he has stated that the changes to the governance of the ICO is positive for the UK data protection regime.[215]

> Our governance arrangements will be modernised to a board and chief executive model. This will enhance our resilience and diversity at senior decision-making level. His Majesty will appoint the Chair of the board via Letters Patent, the same process used for my appointment. As we proposed, the Chief Executive will be appointed by The Chair and Board, rather than the Secretary of State. This will avoid any perceived conflict of interest that could have occurred.[216]

Edwards places significant emphasis on the benefits of Parliamentary accountability and CJEU case law recognises that the 'absence of any parliamentary influence' over supervisory authorities is 'inconceivable'.[217] Indeed, the CJEU states that 'the management of the supervisory authorities may be appointed by the parliament or the government'.[218] The new structure and appointment process for the regulator are highly unlikely to raise any adequacy concerns.

---

[214] DCMS, 'Data: A New Direction – government response' (n 195).
[215] ICO, 'Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill)' (2023) 6 <https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf>.
[216] ibid.
[217] Case C-518/07, *Commission v Germany* ECLI:EU:C:2010:125 para 43.
[218] ibid, para 44.

The Bill also foresees a shift in the regulator's statutory duties. The amended duties of the Commission are set out in Clause 29 DPDI (No 2) Bill[219] as follows:

> 120A Principal objective
> It is the principal objective of the Commissioner, in carrying out functions under the data protection legislation—
> (a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and
> (b) to promote public trust and confidence in the processing of personal data.

Taken in isolation, this does not appear to constitute a notable change from the text of Section 2(2) of the Data Protection Act 2018 which states that:

> (2) When carrying out functions under the UK GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.[220]

More significantly, the proposed Bill identifies some additional duties that must be considered by the Commission when assessing the envisioned role for the reformed supervisory authority. Specifically, Clause 29 DPDI (No 2) Bill proposes the insertion of certain 'duties in relation to functions under the data protection legislation' into the 2018 Act:

> 120B Duties in relation to functions under the data protection legislation
> In carrying out functions under the data protection legislation, the Commissioner must have regard to such of the following as appear to the Commissioner to be relevant in the circumstances—

[219] Intending to amend Part 5 of the Data Protection Act 1998 with the proposed insertion of s. 120A.
[220] Data Protection Act 2018, s. 2(2). Although the inclusion of the promotion of 'public trust and confidence' in data processing could represent a shift if not tied to strong coexistent protections. See also section 4.3 Enforcement Priorities and Record below.

(a) the desirability of promoting innovation;

(b) the desirability of promoting competition;

(c) the importance of the prevention, investigation, detection and prosecution of criminal offences;

(d) the need to safeguard public security and national security.

While each of these interests could be argued to fall under the previously provided for 'interests of data subjects, controllers and others and matters of general public interest', the specific reference to aims including competition and innovation can be viewed as representing a shift in the intended focus of the supervisory authority. This is particularly the case in light of the language used by the government in setting out its plans and vision for the future of data protection in the UK.[221] Introducing these duties could arguably be considered to be the imposition of government priorities onto the supervisory authority, particularly as the Bill requires these priorities to form part of the strategic plan.[222] While the change is concerning from the perspective of prioritising the enforcement of data protection law and the protection of data subject rights, it is worth noting that in response to the initial proposals set out in *Data: A New Direction*, the then Information Commission, Elizabeth Denham noted that the 'requirements to uphold principles such as economic growth, competition, public safety and regulatory cooperation build on our existing work'.[223] The Explanatory Notes to the Bill label these 'new duties', thereby confirming that they were at most implicit considerations for the regulator in the existing regime.[224] The risk this Clause creates is that it will give the regulator cause to prioritise innovation and competition over fundamental rights in situations where there is a tension between the differing priorities.

---

[221] ICO, 'Response to DCMS Consultation "Data: A New Direction"' [2021] <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf>.

[222] Cl. 29 s. 120C.

[223] ICO, 'Response to Data: A New Direction' (n 222) 22. See also: ICO, 'Draft Regulatory Action Policy' 10 <https://ico.org.uk/media/about-the-ico/consultations/4019400/regulatory-action-policy-2021_for-consultation.pdf> .

[224] Data Protection and Digital Information Bill: Explanatory Notes' [2022] Bill 143–EN 30 <https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf>,45, para 259.

As mentioned above, Clause 29 provides for the requirement of the Commission to prepare and publish a strategy.[225] Under the Bill, the Commissioner would be required to consult with other regulators about how its functions are exercised under the data protection legislation that may affect economic growth, innovation, and competition.[226]

More significantly, from the perspective of supervisory independence, Clause 30 of the DPDI (No 2) Bill sets out an important role for the Secretary of State in the setting of 'strategic priorities'. The Bill provides for the designation of a statement of strategic priorities by the Secretary of State that sets out the strategic priorities of the Government relating to data protection.[227] The statement must be laid before Parliament before being designated as the statement of strategic priorities.[228] Following that process, the Commissioner must 'have regard' to the statement when carrying out functions under the data protection legislation – except where the Commissioner is carrying out functions in relation to a 'particular person, case or investigation'[229] – and must explain in writing how this will be done.[230] In addition to a required review after a period of 3 years, the Secretary of State may review the statement of strategic priorities at other relevant times, notably where a Parliamentary general election has taken place or a significant change in Government data protection policy has occurred.[231] Clause 31 amends the provisions of the Data Protection Act 2018 providing for the preparation of codes of practice by the Commissioner giving guidance as to good practice in the processing of personal data.[232] Most notably, the DPDI (No 2) Bill outlines a strengthened role for the Secretary of State in this process, requiring the Commission to consult with the Secretary – and others[233] – on these

[225] By way of the insertion of s. 120C into Data Protection Act 2018.
[226] By way of the insertion of s. 120D into Data Protection Act 2018.
[227] By way of the insertion of s. 120E into Data Protection Act 2018.
[228] Cl. 30 s. 120H.
[229] This exception would be provided for by way of the insertion of s. 120F into Data Protection Act 2018.
[230] This will be required by way of the insertion of s. 120F into Data Protection Act 2018.
[231] Cl. 30 s. 120G.
[232] Cl. 31 s. 124A.
[233] Where the Commissioner considers it appropriate, trade associations, data subjects, and persons representing the interests of data subjects must also be consulted: cl. 31 s. 124A.

codes.[234] Importantly, the Secretary of State is empowered to review and lay codes before Parliament if they approve the codes.[235] If, however, the Secretary of State does not approve a code they are simply required to inform the Commissioner and explain the reasons by way of a statement and publish that statement. In response to this, the Commissioner must revise the code of practice in light of the Secretary of State's statement. This represents a significant change from the 2018 DPA where the Commissioner submits the 'final version' of a code they have prepared[236] to the Secretary of State who is then obliged to lay the code before Parliament.[237] Under current law, the Commissioner then issues the code if, following a 40-day period, neither House of Parliament resolves to not approve the code prepared. If either House resolves to not approve the code, the Commissioner cannot issue the code and must revise it. The 2018 Act makes provision for parliamentary accountability while also empowering the Commissioner as the expert body best positioned to set out the content of the code.

While the CJEU recognises that independence of the supervisory authority must be reconciled with the democratic accountability of the regulator, the combined impact of the changes proposed by the DPDI (No 2) Bill on the independence of the regulator violate the standard for independence set by the CJEU. The GDPR does not specify the strategic priorities of the DPAs, likely because such specification would interfere with their independence[238] Giving control over such priorities to the Secretary of State where Government data protection policy has changed not only unsettles the fundamental rights orientation of the law but directly politicises its application. Allowing

---

[234] Cl. 31 s. 124A.

[235] Cl. 33 s. 124D.

[236] As prepared under Data Protection Act 2018, ss. 121, 122, 123 or 124. See also section 128 'other codes of practice' which are subject to the negative resolution procedure. Section 128 DPA 2018 would be omitted under the DPDI (No 2) Act, but section 124A inserted to provide for 'other codes of practice'.

[237] Data Protection Act 2018, s. 125.

[238] Hijmans suggests that 'this silence is the logical consequence of the complete independence as laid down in Article 8 Charter and Article 16 Treaty on the Functioning of the European Union (TFEU) and underlined in the case law of the Court of Justice of the EU (CJEU).' See Hielke Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? A Reaction to Christopher Hodges' [2018] 1 European Data Protection Law Review 80, 80.

the Government of the day, through the Secretary of State, to veto codes of practice proposed by the regulator, without any parliamentary input, further politicises the application of the law. Such politicisation interferes with the 'complete independence' of the regulator, required by Article 8(3) EU Charter and Article 16 TFEU and described by the CJEU as an 'essential component' of the right to data protection. In settled jurisprudence, now codified in the GDPR, the CJEU considers that independence requires 'decision-making power independent of any direct or indirect external influence on the supervisory authority'.[239] Moreover, in a case concerning the Austrian supervisory authority, the CJEU states that the requirement for independence is intended to 'preclude not only direct influence, in the form of instructions' but also 'any indirect influence which is liable to have an effect on the supervisory authority's decisions.[240] It is difficult to reconcile the role foreseen for the Secretary of State in strategic priority setting and blocking the adoption of codes of practice with such freedom from influence.

4.3 Ensuring Cheap and Effective Individual Remedies

According to the EDPB adequacy criteria, as applied by the Commission, an adequate data protection framework must offer individual remedies and redress mechanisms so individuals can can enforce their rights 'rapidly and effectively, and without prohibitive cost'.[241] The DPDI (No 2) Bill changes the procedures for complaint handling by the Information Commission in a way that materially alters the availability of individual remedy and redress. The data subject's right to lodge a complaint with a supervisory authority and the corresponding enforcement duty of that authority are considered to be crucial mechanisms for accountability and individual empowerment in data

[239] *Commission v Germany* (n 217) para 19. Similarly, Convention 108+ – which is referenced in the UK adequacy decision – states that 'supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions'. Convention for the protection of individuals with regard to the processing of personal data. Convention 108+, art. 15(5).

[240] Case C-614/10 *Commission v Austria* ECLI:EU:C:2012:631, para 43.

[241] A29WP, 'WP254' (n 4) 8.

protection law.[242] The DPDI (No 2) Bill proposals would remove the 'right to lodge a complaint with the Commissioner' as provided for in Article 77 UK GDPR.[243] References to this provision would be replaced by references to Sections 165 and 164A DPA 2018 as amended by the DPDI (No 2) Bill. Section 165 DPA 2018 concerns complaints by data subjects to the ICO and the proposed 164A DPA 2018 would address complaints by data subjects to controllers.[244] On its face, the newly proposed Section 164A appears to be a positive development for data subject rights as it requires controllers to facilitate the making of complaints, to acknowledge complaints within thirty days of receipt, to 'take appropriate steps to respond' without undue delay, and to 'inform the complainant of the outcome'. Section 164A should not be considered in isolation, however, as it interacts with proposed amendments to the ICO complaints procedure in an important manner.

The proposed Clause 42 of the DPDI (No 2) Bill is titled, 'Power of the Commissioner to refuse to act on certain complaints'. To understand the changes proposed in this clause, it is necessary to consider what the current law requires. The DPA 2018 obliges the Commissioner to take 'appropriate steps' to respond to complaints.[245] 'Appropriate steps' include investigating the complaint to the 'extent appropriate' and informing the complainant about progress.[246] This reflects the GDPR obligation where supervisory authorities are required to 'handle' complaints 'with all due diligence'[247] and to investigate 'to the extent appropriate'.[248]

---

[242] Recital 141 GDPR. Access Now and Data Protection Law Scholars Network, 'The right to lodge a data protection complaint: OK, but then what? An empirical study of current practices under the GDPR'[2022] <https://www.ivir.nl/publicaties/download/GDPR-Complaint-study-1.pdf>, 9.
[243] Schedule 8.
[244] Cl 41.
[245] Data Protection Act 2018 s.165(4).
[246] ibid s. 165(5).
[247] *Schrems II* (n 95) para 109.
[248] Article 57(4) GDPR. The interpretation of 'to the extent appropriate' under the GDPR varies and some supervisory authorities have interpreted it to mean 'that they are not obliged to produce a decision in all circumstances and can instead resort to the amicable settlement of disputes or even to switch to own initiative inquiries in the course of complaint-handling.' Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' [2022] 71 International & Comparative Law Quarterly 799, 821.

The DPDI (No 2) Bill proposes a new limitation to the requirement in UK law to take 'appropriate steps' and provides for an authority to 'refuse to act' if one of three conditions are met:

> 165A Power of Commissioner to refuse to act on certain complaints
>
> (1) The Commissioner may refuse to act on a complaint under section 165 if condition A, B or C is met.
> (2) Condition A is that—
> (a) the complaint concerns an infringement of the UK GDPR or Part 3 of this Act, and
> (b) the complaint has not been made to the controller under section 164A.
> (3) Condition B is that—
> (a) the complaint has been made to the controller under section 164A,
> (b) the controller has not finished handling the complaint in accordance with subsection (4) of that section, and
> (c) the period of 45 days beginning with the day the complaint was made to the controller under that section has not expired.
> (4) Condition C is that the complaint is vexatious or excessive (see section 204A).[249]

If the Commissioner refuses to act on a complaint, they must inform the complainant of the refusal, the reasons for it, and the right to appeal the decision to the Tribunal.[250]

The new power to refuse to act on certain complaints, appears to be a departure from the text of the GDPR,[251] where Article 77 provides data subjects with the right to lodge

---

[249] Cl 42.

[250] ibid. Section 166A provides that: '(1) Where the Commissioner refuses to act on a complaint in reliance on section 165A, the person who made the complaint may appeal to the Tribunal. (2) The Tribunal may review any determination of fact on which the refusal to act was based. (3) If the Tribunal considers— (a) that the refusal to act is not in accordance with the law, or (b) that the Commissioner ought not to have exercised the discretion to refuse to act, the Tribunal must allow the appeal. (4) Otherwise, the Tribunal must dismiss the appeal.'

[251] And the retained UK GDPR in its current form, although amendment to this is envisioned in the DPDI (No 2) Bill.

a complaint with the relevant supervisory authority 'if the data subject considers that the processing of personal data relating to him or her' infringes the GDPR.[252] The first two conditions (Condition A and B) of the proposed Section 165A DPDI (No 2) Bill impose procedural requirements on the data subject to engage with the controller before a complaint can be made to the Commission.[253] This is a dilution of the right to lodge a complaint with a supervisory authority and may have implications for the speed with which certain complaints are addressed.[254] It also has the potential to undermine future investigations if advance knowledge of the complaint is abused by controllers. While such a requirement undoubtedly weakens the rights of data subjects, it is unclear whether it would be deemed problematic by the Commission. Evidence suggests that several EU DPAs have informally adopted a similar stance and will only consider complaints once they have been raised first with the controller.[255]

Condition C, which empowers the Commissioner to refuse to act if a complaint is 'vexatious or excessive', requires further consideration.[256] The DPDI (No 2) Bill would amend the UK GDPR by the addition of 'excessive' and 'vexatious' to the index of defined expressions in Section 206 UK GDPR. Provision is made for the insertion of a reference to the proposed Section 204A for each term.[257] The proposed Section 204A – as subsequently amended by Schedule 8 of DPDI (No 2) Bill – states that:

> whether a complaint to the Commissioner is vexatious or excessive must be determined having regard to the circumstances of the complaint, including (so far as relevant)—

---

[252] Article 77 GDPR. Moreover, the GDPR requires supervisory authorities to handle complaints and to 'investigate, to the extent appropriate' the subject matter of complaints and inform complainants of the progress and outcome of investigations within a reasonable period. ibid, art. 57(f). Articles 57 and 77 GDPR were both retained in UK GDPR, although changes are proposed in DPDI (No 2) Bill.

[253] Cl. 41 s. 164A.

[254] Notably, the data subject may be required to wait up to thirty days for a simple 'acknowledgement' of their complaint at the first stage of making a complaint to the controller under the proposals.

[255] Access Now, 'The right to lodge a data protection complaint' (n 242) 44-45.

[256] The proposed section 165A(5) as contained in clause 42 of the DPDI (No 2) Bill states that 'In any proceedings where there is an issue as to whether a complaint is vexatious or excessive, it is for the Commissioner to show that it is'. Cl. 42, s. 165A.

[257] ibid, cl. 8(11).

(a) the nature of the complaint,
(b) the complainant's relationship with the person who is the subject of the complaint ("the subject") and the Commissioner,
(c) the resources available to the Commissioner,
(d) the extent to which the complaint repeats a previous complaint made by the complainant to the subject or the Commissioner,
(e) how long ago any previous complaint was made, and
(f) whether the complaint overlaps with other complaints made by the complainant to the subject or the Commissioner.[258]

For the purposes of the Act, examples of complaints that may be vexatious include complaints that:

(a) are intended to cause distress,
(b) are not made in good faith, or
(c) are an abuse of process.[259]

If the ICO refuses to act on a complaint on the basis that it is 'vexatious or excessive', the DPDI (No 2) Bill would require the Commissioner to demonstrate that this is the case in any proceedings where there is an issue.[260] According to the Explanatory Notes, this change 'aligns with the same change in threshold being made across the UK GDPR and DPA 2018'.[261] Elsewhere in the Explanatory Notes, it is suggested that this threshold sets a lower bar for the refusal to deal with requests and complaints than the existing threshold.[262] Moreover, it is difficult to see why 'the resources available to the Commissioner' should be part of the circumstances to be considered when determining whether a complaint to the Commissioner is vexatious or excessive. As pointed out by the Open Rights Group in the context of the same consideration being

[258] ibid, sch 8. This would be s. 204A(1A).
[259] ibid, sch 8. This will be s. 204A(2).
[260] ibid cl 42 s165A.
[261] Explanatory Notes (n 224) 50, para 311.
[262] Explanatory Notes (n 224) 30.

applied to controllers, 'a lack of resources or organisational preparedness to deal with a request does not indicate inappropriate use of data protection rights'.[263]

When considering whether the proposed changes would offer protection that is essentially equivalent to that offered under EU law, it is important to consider what standards apply across Europe. The GDPR's obligation to 'handle' complaints only applies to complaints that are 'deemed admissible'.[264] According to an internal EDPB document, inadmissible complaints generally entail situations where 'the subject matter of the complaint is clearly not related to the protection of personal data'; 'the claim is manifestly unfounded or excessive pursuant to Article 57.4 of the GDPR';[265] or 'the claim does not fulfil the formal conditions laid down by the Member State of the SA which received the complaint'.[266] The shift is therefore one from manifestly unfounded or excessive complaints to a standard of vexatious or excessive. The loss of the adjective manifestly suggests a lower standard for the refusal to handle complaints. Moreover, the way in which the Bill defines vexatious appears to depart from the interpretation of that term in other contexts. For instance, in jurisprudence concerning vexatious litigation and litigants, the High Court has held that the hallmark of a vexatious claim is that it has 'little or no basis in law' and that its 'effect is to subject the defendant to inconvenience, harassment and expense out of all proportion to any gain likely to accrue to the claimant'.[267] The High Court has also confirmed that the rationale for preventing vexatious claims is not to 'prevent access to the courts' or to 'prevent applicants bringing applications which fail'. Rather, it is to prevent 'the

---

[263] Open Rights Group, 'Analysis: The UK Data Protection And Digital Information Bill 19 October 2022' 15. Open Rights Group further suggest that the amendments give clear discretion to the ICO to refuse to act on complaints by making assumptions about the motives of the complainant. ibid 19.

[264] Access Now, 'The right to lodge a data protection complaint' (n 242) 4.

[265] Article 57(4) GDPR states that 'Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.'

[266] EDPB, 'Internal EDPB Document 6/2020 on Preliminary Steps to Handle a Complaint: Admissibility and Vetting of Complaints' 6 <https://edpb.europa.eu/our-work-tools/our-documents/internal-documents/internal-edpb-document-62020-preliminary-steps_en>.

[267] *Attorney General v Barker* [2000] EWHC 453 (Admin), para 19 (Lord Hoffman).

persistent bringing of applications which are hopeless'.[268] This substantive element – little or no basis in law, or hopelessness as a claim – are absent from the criteria for vexatious complaints in the Bill. This leaves the prospect open that complaints which have substantive merit will be rejected by the Commissioner on these grounds. This concern is borne out by the comments of Government and the Information Commissioner. In its response to the 'Data: A New Direction' consultation, the Government stated its desire to refocus the Commissioner's statutory commitments 'away from handling a high volume of low-level complaints, and towards addressing the most serious threats to public trust and inappropriate barriers to responsible personal data use'.[269] The Department then responsible for the legal reform (then DCMS; now SIT) described the proposed changes as clarifying the flexibility of the ICO as to how they investigate complaints.[270] It suggested that this increased clarity would enable the ICO 'to exercise discretion with greater confidence' in a manner that would 'allow the ICO to investigate complaints in a more agile, risk-based way'.[271] The Information Commissioner Edwards suggested that these changes will 'free up more resources to focus on tackling the greatest harms to people and issues where we can have the biggest impact'.[272] Both the wording of the proposed changes in the Bill as well as these statements prior to its adoption indicate that its aim is to shift the focus of the regulator away from individual complaint-handling to more strategic applications of the law. There is evidence to suggest that some EU Member States have 'expanded the possibilities for DPAs to reject complaints on grounds not foreseen under the GDPR'[273] and engage in the strategic enforcement of the law.[274] Nevertheless, it is

---

[268] *Crimson Flower Productions Ltd v Glass Slipper Ltd* [2020] EWHC 942 (Ch).
[269] DCMS, 'Data: A New Direction – government response' (n 195) chap 5.1.
[270] The scope of the discretion to investigate to the 'extent appropriate' is considered in *Killock & Veale & others v Information Commissioner* (GI/113/2021 & others).
[271] DCMS, 'Data: A New Direction' (n 193) 133.
[272] ICO, 'Response to the DPDI No 2 Bill' (n 215) 6.
[273] EDPB, 'Document 6/2020' (n 266) 14.
[274] Orla Lynskey, 'General Report Topic 2: The New EU Data Protection Regime' 23, 60. Available at: http://real.mtak.hu/129207/1/FIDE_OA_vol_2.pdf

possible that such approaches to complaint-handling by supervisory authorities are themselves incompatible with EU law.

This raises the related point of whether the UK's data protection system would then 'ensure a good level of compliance' as required by the EDPB's adequacy criteria. A good level of compliance entails accountability and awareness amongst controllers and processors and recognition that 'sanctions and supervision have an important role in ensuring respect for the rules'.[268]

The enforcement record of the ICO – even following the strengthening of its powers post-GDPR – has been the subject of criticism.[275] Erdos has compiled information from the ICO annual reports that provides insight into the complaints handling and substantive enforcement actions undertaken (see the modified table below). Erdos describes the record as demonstrating a 'very low' 'intensity of enforcement'.

[275] Victoria Hewson and James Tumbridge, 'Who Regulates the Regulators? No. 1: The Information Commissioner's Office' [2020], 4. Available at <https://iea.org.uk/wp-content/uploads/2020/07/Who-regulates-theregulators_.pdf> ; Open Rights Group, 'Data Regulator ICO Fails to Enforce the Law' [2020], https://www.openrightsgroup.org/press-releases/data-regulator-ico-fails-to-enforce-the-law/.

Table 1: Annual Summary of ICO Complaint Handling and Enforcement Actions (2018-2022)[276]

Year	Data Protection Complaints Handled	No Infringement Finding	Infringement Finding	Reported Substantive Data Protection Enforcement
2018-2019	34,684	11,411	9,503	22 fines (total £3.01m)
2019-2020	39,890	18,136	10,044	2 Enforcement Notices 15 Fines 8 Prosecutions 5 Cautions
2020-2021	31,008	Not disclosed	Not disclosed	3 fines (total £39.65m) 1 Enforcement Notice
2021-2022	41,088	Not disclosed	Not disclosed	4 fines (total £633k) 24 reprimands

The 2022-2023 ICO report, published after Erdos' analysis, notes that 39,724 data protection cases were handled but little specific detail is provided. In a table reporting the 'High level outcomes' for 2022-2023, it is indicated that in 64.95 per cent of cases, advice was given, but no further action was taken; in 35.02 per cent of cases, informal

[276] This is a modified version of a table originally produced in David Erdos, 'Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans', University of Cambridge Faculty of Law: Paper No 16/2022, 14.

action was taken; and in 0.03% of cases some 'other' outcome was reached.[277] Little detail is provided about fines, but the report notes that £15.271 million was imposed in monetary penalties. This includes fines related to infringements of other laws, such as the Privacy and Electronic Communications Regulations. The ICO website database of enforcement action provides some additional insight. From the 1 April 2022 to 31 March 2023, 34 monetary penalties are recorded.[278] The majority of the monetary penalties for the year are related to direct marketing and thus should not be considered as part of the data protection stricto sensu fines. Notwithstanding this, the cumulative fines issued relating to infringements under the GDPR totalled £13,379,200. These fines were distributed across just five cases, with £7,552,800 of that total relating to a fine against Clearview AI in May 2022.[279]

In light of this, it is necessary to briefly consider how the ICO has exercised its discretion under current law. One notable example has been the ICO approach to enforcement against public authorities and financial penalties. In an open letter to public authorities in June 2022, Commissioner Edwards set out a 'revised approach to working more effectively with public authorities across the UK'. This approach, which Edwards noted would be trialled for two years, would see a greater use of his discretion in issuing fines to public authorities.[280] According to Edwards:

> In practice this will mean an increase in public reprimands and the use of my wider powers, including enforcement notices, with fines only issued in the most egregious cases. However, the ICO will continue to investigate data breaches in the same way and will follow up with organisations to ensure the required

[277] ICO, 'Information Commissioner's Annual Report and Financial Statements 2022/23, July 2023 HC 1440' 56 <https://ico.org.uk/media/about-the-ico/documents/4025864/annual-report-2022-23.pdf>.
[278] ICO, 'Enforcement Action' [2022] <https://ico.org.uk/action-weve-taken/enforcement/> .
[279] ibid ; ICO, 'Clearview AI Inc.' [2022] <https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/>.
[280] While not directly related to the issue of ICO discretion, it should be noted that the GDPR provides Member States with flexibility on whether and to what extent administrative fines may be imposed on public authorities in their jurisdiction. Article 83(7) GDPR.

> improvements are made. We will also do more to publicise these cases, sharing the value of the fine that would have been levied, so there is wider learning.[281]

In spite of Edwards' explanation,[282] the approach has been criticised, including for the lack of consultation ahead of its introduction.[283] Since the adoption of the new approach, Baines suggests that the ICO seems less inclined to issue fines as a general matter, including against non-public authorities.[284] Baines draws attention to the deterrent effect of fines as assessed by Upper Tribunal Judge Mitchell:

> I do not think it can be sensibly disputed that, in general, the prospect of significant financial penalties for breach of data protection requirements makes a controller or processor more likely to eschew a lackadaisical approach to data protection compliance and less likely to take deliberate action in breach of data protection requirements.[285]

In this context it is worth reflecting on Erdos' point that

> There is an understandable targeted rationale for the core of many of the concrete proposals put forward in the DPDI Bill. Nevertheless, certain caveats to this must be emphasised not least since as currently drafted some risk providing a de jure entrenchment of the ICO positioning away from being a comprehensive upholder of core data protection rights.[286]

---

[281] ICO, 'How the ICO Enforces: A New Strategic Approach to Regulatory Action' [2022] <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/how-the-ico-enforces-a-new-strategic-approach-to-regulatory-action/>.

[282] ibid.

[283] Jon Baines, 'Has ICO "No Fines" Policy Been Introduced without Proper Debate?' (informationrightsandwrongs, 28 July 2023) <https://informationrightsandwrongs.com/2023/07/28/has-ico-no-fines-policy-been-introduced-without-proper-debate/>.

[284] ibid.

[285] ibid.

[286] Erdos, 'Towards Effective Supervisory Oversight?' (n 276) 3.

4.4 Onward Transfers of Personal Data

Article 45(2) GDPR specifically provides that the Commission must take account of 'rules concerning onward transfers' when conducting adequacy assessments. This is also reflected in the EDPB's Adequacy Referential (WP254) which features "restrictions on onward transfers" amongst the content principles that must be considered in adequacy assessments. It specifies that onward transfers of data should only take place for limited and specified purposes and as long as there is legal ground for that processing.

This concern for onward transfers was manifest in the existing UK adequacy decision process. In its Opinion, the EDPB highlighted the risk that onward transfers from the UK to third countries might undermine the protection offered to data,[287] highlighting six particular challenges.[288] Several of these relate to the way in which the UK will assess adequacy for onward transfers under its data protection framework. For instance, the EDPB advised the Commission to monitor the criteria taken into account in future adequacy assessments and when applying the derogations provided for in the UK GDPR. It also noted that the UK had recognised as adequate the third countries that were deemed adequate under the old Directive although the Commission had yet to review these adequacy decisions.[289] A further concern was about the standards applied when appropriate safeguards are used as the legal basis for data transfers. Here, the EDPB suggests that data exporters must nevertheless assess on a case-by-case basis the legal framework of the third country and introduce any supplementary measures necessary to ensure essentially equivalent protection.[290] In essence, the EDPB considered it necessary that onward data transfers meet the *Schrems II* conditions.

[287] EDPB, 'Opinion 14/2021' (n 164) para 14.
[288] ibid, paras 79 to 106.
[289] ibid, para 16.
[290] ibid, para 84.

The EDPB Opinion paid particular attention to the relationship between onward transfers and international agreements entered into by the UK. It expressed 'strong concerns' regarding the existing UK-US Cloud Act Agreement.[291] This agreement lays down conditions for direct access by US authorities to data in the UK as well as conditions in which UK data controllers and processors can transfer data to US authorities.[292] The EDPB recommended that the Commission fulfil its monitoring role and where essential equivalence is not maintained, it should 'consider amending the adequacy decision to introduce specific safeguards for data transferred from the EEA and/or to suspend the adequacy decision.'

The Commission's adequacy decision stresses that the application of the UK rules on international transfers is an important factor to ensure the continuity of protection in case of EU-UK data transfers.[293] The Commission appeared confident that the existing measures (adequacy, contractual measures and derogations) would not undermine essentially equivalent protection. The Commission therefore simply committed to 'closely monitor the situation' in the UK to assess whether the various transfer mechanisms are used in a way that ensures continuity of protection.[294] The Commission was similarly assured that data transferred to US authorities under the UK-US agreement would benefit from equivalent protection. The Agreement explicitly provides that it will offer equivalent protection to that provided by the EU-US Umbrella agreement, although the details of the concrete implementation of the agreement were yet to be determined.[295] The Commission requested further information and clarification on these safeguards as soon as they became available.[296]

---

[291] ibid.

[292] The EDPB appeared unconvinced that the explanations provided by the UK government around data access or the claim that the data would benefit from the same protection as that afforded by the EU-US Umbrella agreement would be binding in domestic law or would contain the specific safeguards required for essential equivalence. ibid, paras 88-92.

[293] Commission Implementing Decision 2021/1772/ EU (n 113) recital 74 and 82.

[294] ibid, Recital 82.

[295] ibid, recitals 154 and 155.

[296] ibid, recital 155.

Turning to the changes proposed in the DPDI (No 2) Bill, Clause 23 amends Chapter 5 of the UK GDPR via Schedule 5. The mechanism for third country transfers will still include appropriate safeguards per Article 46 GDPR and the derogations under Article 49. However, the Article 45 provision on adequacy is replaced with a new Article 45A entitled 'Transfers Approved by Regulations'. Under this provision, the Secretary of State can make regulations for transfers to third countries, taking into account matters including the desirability of the data transfer subject to a new "data protection test" found in Article 45B. This new test bears a resemblance to an adequacy assessment as, rather than requiring essential equivalence, it requires that the third country protections are 'not materially lower than those offered in the UK'. Notably absent amongst the list of elements that the Secretary of State must consider are the rules concerning data access and use by public authorities for purposes including national security and law enforcement agencies in the third country and the requirement of independent oversight of data protection law.[297] It is also notable that the third country must offer arrangements for judicial or non-judicial redress for data subjects, meaning that judicial redress in the third country will not be required. The Secretary of State may approve transfers by means of 'sector, controller, recipient, specific data or schemes' amongst other areas. The aim of this new approach is to enable more targeted data transfers, taking into consideration the risk to the specific data transferred rather than from the entire legal regime of the third country. However, there will be instances where these two are inseparable, such as where the data is transferred to a third country where national security access is permitted under conditions that would not meet EU standards or where the oversight of data protection law is heavily politicised. Such transfers would appear, in principle, to be possible pursuant to the new data protection test.[298]

[297] Article 45B(2)(a)-(f) found in Schedule 5.

[298] Similar changes apply to the transfer of personal data to third countries for law enforcement purposes. See, Article 74AA and 74AB.

Beyond these changes found in the DPDI (No 2) Bill it is worth noting that the UK has recognised South Korea as adequate[299] and has recently confirmed the UK-US 'data bridge" described as a "UK extension to the EU-US Data Privacy Framework'.[300] These agreements align directly with the adequacy decisions of the EU. However, the UK government has previously announced that it would prioritize data transfer and sharing agreements with several countries not yet recognised as adequate by the EU (including Australia, Brazil, Colombia, Dubai, Kenya, India and Indonesia).[301]

In practice, the EDPB in its Opinions and the Commission in its assessments have paid particular attention to the rules concerning onward transfers. Supplementary rule 4 was added to the Japanese adequacy decision to augment protection while the EU-U.S. DPF contains an 'accountability for onward transfer principle'.[302] The latter principle ensures that any onward transfers from the data recipient in the US, whether within the US or to a third country, can only take place for limited and specified purposes on the basis of a contractual arrangement that requires the third party to provide the same level of protection as that guaranteed by the Principles.[303] This suggests that the changes introduced by the DPDI (No 2) Bill would be closely scrutinised for their compliance with EU requirements.

4.5 Changes to the Rights of Individuals and other Societal Safeguards

In addition to the changes outlined above to the rights of individuals before the regulator, the Bill proposes to change the existing rights of individuals in small but potentially significant ways and to alter the societal safeguards provided by the data

---

[299] The Data Protection (Adequacy) (Republic of Korea) Regulations 2022.
[300] UK Government Notice, 'UK-US data bridge: joint statement' [2023] https://www.gov.uk/government/publications/uk-us-data-bridge-joint-statement
[301] UK Government Press Release, 'UK unveils post-Brexit global data plans to boost growth, increase trade and improve healthcare' [2021] https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare
[302] See Annex I, Section II.3 and Supplemental Principle 'Obligatory contracts for Onward Transfers' (Annex I, Section III.10).
[303] Recital 37.

protection framework. While not exhaustive, three key changes are of note: (i) the removal of the prohibition on automated decision-making; (ii) restrictions on the rights of data subjects; and (iii) consequential changes to data protection impact assessments (DPIAs).

(i) The Removal of the Prohibition on Automated Decision-making

Clause 12 of DPDI (No 2) Bill replaces the current prohibition on automated decision making found in Article 22 with a new Section 4A. While the existing provision prohibits solely automated decision making that has a legal or similarly significant effect on the individual, subject to some exceptions, the new provision limits this prohibition to automated decision-making based on sensitive data processing alone. In other words, solely automated decision making that would significantly impact the individual is permitted because of this revision. However, many impactful automated decisions are made without relying on sensitive data, including the type of automation that led to the A-level algorithm scandal or the assessment of creditworthiness conducted to make decisions regarding access to financial products. Where a significant decision is made about an individual through solely automated means, safeguards nevertheless continue to apply. The data subject must be provided with information about the decision and be able to make representations about it, to obtain human intervention and to contest the decision.[304]

It is the Secretary of State who is given the power to define by regulations what constitutes meaningful human involvement in a decision; what decisions have a similarly significant effect to a legal effect on an individual; and what safeguards are satisfactory for such decision making.[305] The full impact of the changes to the law will not therefore be tangible until such regulations are adopted. Nevertheless, the change represents a material diminution of the level of existing protection to fundamental rights in the context of automated decision making. Nevertheless, taken in isolation it appears unlikely to lead to a finding by the Commission that the UK's legal framework does not

[304] Article 22C(2)(a)-(d).
[305] Cl 12, Article 22D.

offer essentially equivalent protection. This is for two reasons. First, the regulation of automated decision-making has not featured heavily in the adequacy decisions adopted by the Commission to date. The A29WP had explicitly encouraged the Andorran authorities to adopt new legislation to address automated decision making[306] while the lack of protection for individuals in the context of automated decision-making in New Zealand was accepted as the 'expert report makes clear that automated decision making is not common in New Zealand and there are various rules to discourage the practice.'[307] This lack of emphasis may be explained in part by the fact that provisions explicitly addressing automated decision-making were notably absent in the older generation of data protection laws. To the extent that newer, modernised iterations tend to include such provisions the Commission may be more attentive to them in future adequacy decisions. Secondly, it is then significant that the UK appears to continue to meet the standards required by the Council of Europe's data protection convention, Convention 108+, for automated decision-making.[308] Article 9 Convention 108+ provides that data subjects have a right not to be subject to a decision significantly affecting them based solely on an automated processing of data without having his or her views taken into consideration. The proposed revisions do extend this safeguard – the right to have their views taken into consideration – to data subjects. The explanatory memorandum to Convention 108+ elaborates on the rationale for this requirement. This provision provides the data subject with the opportunity to substantiate the possible inaccuracy or irrelevance of the data used, or to highlight other factors that might impact upon the result of the decision making.[309]

---

[306] European Commission, Implementing Decision 2010/625/EU, recital 14.

[307] Opinion 11/2011, 12.

[308] Erdos similarly considers that this reformulation 'would appear broadly in line with the Article 9(1)(a) of the DPC+'. David Erdos, 'A Bill for Change? Analysing the UK Government's Statutory Proposals on the Content of Data Protection and Electronic Privacy', University of Cambridge Faculty of Law: 13/2022, 17.

[309] Council of Europe, 'Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data', 24. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

(ii) Restrictions on the Rights of Data Subjects

Clause 8 of the Bill concerns 'vexatious or excessive' requests by data subjects. Clause 8(3) inserts into the UK GDPR a new Article 12A. Article 12A allows controllers to charge a reasonable free, or to refuse to act upon, data subject requests under Articles 15-22 and 34 GDPR that the data controller deems to be 'vexatious or excessive'. This replaces the prior standard for refusing data subject access requests that were 'manifestly unfounded or excessive'. The Bill sets out non-exhaustive criteria to take into consideration when determining whether the request is vexatious or excessive. These mirror those set out above to be applied by the Information Commission when refusing to act on complaints deemed vexatious or excessive and include the relationship between the data subject and the controller; the resources available to the controller; and the nature of the request. Requests that are not made in good faith, are on abuse of process or are intended to cause distress are provided as examples of vexatious requests.

The rationale for this change in terminology is unclear. It has been suggested that the term vexatious is used in the Freedom of Information Act 2000 and there may be an intention to align the subject access standards to the Freedom of Information regime.[310] This may be advantageous from the regulator's perspective however there are otherwise significant differences in the two legal regimes: data subject access requests are more narrow in scope (pertaining only to an individual) than FOI requests and can be addressed to both public and private data controllers.[311] It has also been suggested that this change was based on feedback from organisations that this is easier for them to understand'.[312] Whether this is the case remains to be seen. What

[310] Freedom of Information Act 2000, s 14. DCMS, 'Data: A New Direction – government response' (n 195), chapter 2.3.
[311] Open Rights Group, 'Analysis' (n 263) 15.
[312] ICO, 'Response to the DPDI No 2 Bill' (n 215) 3. In Data: A New Direction, DCMS appeared to put particular emphasis on the perceived abuse of subject access requests, noting that 'the general position under current law is that a controller cannot consider the purpose of a subject access request unless it seems apparent that the request is 'manifestly unfounded', whereby the data subject has no intention

is significant from an adequacy perspective is whether this leads to a reduction in the standards of protection offered to individuals. While some suggest that each of the provided examples of vexatious requests 'could easily fit into "manifestly unfounded"', the criteria to interpret vexatious in the Bill could apply well beyond these examples. Indeed, the Explanatory Notes to the Bill state that the new threshold should allow organisations to refuse requests (or charge fees) more easily than under the existing threshold of 'manifestly unfounded or excessive'.[313] It is noteworthy that during parliamentary Committee hearings concerning the Bill, witnesses appearing voiced their concerns about this particular element of the Bill. In particular, it was noted that relevant stakeholders (including the TUC, Which? and the Public Law Project) expressed concerns that, as currently drafted, the new threshold is too subjective and could be abused by controllers who may define requests they do not wish to deal with as vexatious.[314]

(iii) The Abolition of Mandatory Data Protection Impact Assessments (DPIAs)

The Bill will replace DPIAs with 'Assessments of High-Risk Processing' (Clause 18). Such assessments must include (a) a summary of the purposes of the processing, (b) an assessment of whether the processing is necessary for those purposes, (c) an assessment of the risks to individuals, and (d) a description of how the controller proposes to mitigate those risks. As a result of this proposed change, the law will no

---

of exercising their right of access, or where the subject access request is 'malicious in intent' and is 'being used to harass an organisation with no real purpose other than to cause disruption'. The government is aware that some organisations believe that the threshold of 'manifestly unfounded' makes it difficult for data controllers either to navigate instances in which it would be appropriate to enquire about the purpose of the request, or to provide sufficient grounds for a refusal to comply with a request.' DCMS, 'Data: A New Direction' (n 193) para 186. In Committee debates it was noted that the Information Commissioner was 'fairly clear on what that terminology means and it will reflect the existing body of law in practice'. 'Public Bill Committee, Data Protection And Digital Information (No 2) Bill, First Sitting Wednesday 10 May 2023 (Morning)' 14 and 7 <https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf>.

[313] Explanatory Notes (n 224) 11.

[314] Public Bill Committee, DPDI (No 2) Bill, Tuesday 16 May 2023, p111. Available at: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf

longer identify the situations in which a DPIA is required[315] nor will it require the controller to seek the views of data subjects where appropriate.[316] The amended provision is also less prescriptive concerning the criteria for evaluating risk and implementing risk mitigation. In determining the impact of this provision, much will depend on how the notion of high risk is defined. However, a major change introduced by the Bill concerns the consultation of the regulator prior to processing. Article 36 UK GDPR provides that controllers shall consult the Commissioner prior to processing, where a DPIA suggests that processing is high risk in the absence of risk mitigation measures. The Bill changes this from an obligation, rendering such prior consultation voluntary.

Convention 108+ also provides for impact assessments, albeit in a far less detailed manner than the GDPR. It requires controllers (and processors, where relevant), prior to processing, to 'examine the likely impact of intended data processing on the rights and freedoms of data subjects'.[317] Parties to the Convention can moreover adapt the application of this provision according to the nature and volume of the data, the nature, scope and purpose of processing and, where appropriate, the size of the controller or processor.[318] The proposed changes in the UK DPDI (No 2) Bill therefore appear to fall within the margin for manoeuvre allowed by Convention 108+ in this regard.

4.6 The Implications for Adequacy: An Appraisal

The previous sub-sections have identified, in a non-exhaustive manner, the most significant changes to UK data protection law for adequacy purposes. Four key concerns were identified. These were the impact of the changes on the independence of the supervisory authority and onward transfers of personal data; the continued availability of cheap and effective individual remedies; and the significance of the reform for individual rights and societal safeguards. To what extent could these

[315] Currently found in Article 35(3) GDPR.
[316] Article 35(9) GDPR.
[317] Article 10(2) Convention 108+.
[318] Article 10(4) Convention 108+.

changes lead to the loss of the UK's adequacy status? As is apparent from Chapter 3, the answer to this question may differ depending on whether it is asked of the European Commission or the CJEU.

As our assessment of adequacy decisions adopted to date by the European Commission reveals, although the Commission should conduct a strict standard of review when adopting decisions[319], it is relatively generous in its approach (compared to the EDPB or the CJEU). This is particularly so when it comes to its review of existing adequacy decisions, as the recent sparse yet positive review of the Japanese adequacy decision indicates. While the UK adequacy decision is distinct due to its sunset clause and its higher political salience, it seems likely that the Commission will endeavour to maintain the UK's adequacy status if feasible. Of the four changes discussed above, the changes to individual rights and redress would likely be treated as within the margin for manoeuvre afforded by adequacy and characterised as a different approach rather than anything more consequential. The possibility of onward data transfers from the UK circumventing EU protection is more likely to be problematic. As noted above, the Commission may require additional safeguards for data of EU provenance to prevent such circumvention (such as those provided in the Japanese adequacy decision and the EU-US Privacy Framework). The most difficult issue for the Commission to deal with concerns the enhanced substantive role of the Secretary of State in data protection law and its impact on the independence of the regulator. While the post-GDPR adequacy decisions do refer to the independence of the oversight provided in third countries, their treatment of this condition has not been very detailed. As a result, it is difficult to predict how the Commission will deal with this change. Unlike onward transfers, the independence concern cannot be easily addressed through assurances, whether in the adequacy decision or annexed to it. It is this politicisation of data protection law that therefore appears to be the biggest threat to the renewal of the UK's GDPR adequacy decision.

[319] *Schrems* (n 83) para 78.

Should a new UK adequacy decision be granted and challenged before the CJEU, there is a bigger risk to its validity as a result of the proposed changes. First, as is apparent from the *Schrems I* and *II* jurisprudence as well as *Opinion 1/15*, the Court adopts a stricter scrutiny lens for adequacy than other EU Institutions and it shows a distinct lack of deference to their appraisals of adequacy. Before the CJEU, the biggest threat to adequacy stems from the changes to the roles of the Information Commissioner and the Secretary of State under the Bill. The role of the Secretary of State appears to fall foul of the requirements for independence set by the Court in *Commission v Austria, Commission v Germany* and *Commission v Hungary*.[320] Moreover, the Court is on record in *Schrems* as stating that the complete independence of the regulator is an essential component of the right to data protection. There is no reason to suggest that the Court would interpret Article 8(3) EU Charter differently in the data transfer context as it would under EU data protection law more generally.[321] As this flaw pertains to the general oversight of the system, it is not easily severable from the rest of an adequacy assessment. This may prove fatal for UK adequacy before the CJEU.

Moreover, as *Opinion 1/15* suggests, the Court is more likely to take a holistic approach to the review of an adequacy appraisal than the adequacy approach adopted by the Commission. In *Opinion 1/15* the Court, contrary to the submissions of the Commission, the Council and all intervening Member States, documented what it considered to be a litany of shortcomings of the EU-Canada PNR agreement in finding that this agreement was incompatible with the EU Charter. It is therefore possible that the Court will also look at the aggregate impact of the changes introduced by the DPDI (No 2) Bill, in particular concerning the right to lodge a complaint with the regulator and the possibility for controllers to refuse to act on requests they deem vexatious, and conclude that the standard of protection offered in the UK falls short of essential equivalence to that in the EU. Commentators in the UK have also emphasised that it

---

[320] *Commission v Germany* (n 217) para 25; C-288/12, *Commission v Hungary* EU:C:2014:237, para 48; and *Schrems* (n 83) para 41.

[321] This is borne out by the *Schrems* case where the Court applied the Digital Rights Ireland interpretation to the context of international data transfers.

is the cumulative effect of the changes that may be most significant. For instance, Pounder suggests that 'as AI alarms become more shrill, the hands on the data protection tiller grow softer'[322] while Erdos highlights that 'discrete changes...remain imperative'.[323] Finally, it is also worth emphasising that should the validity of an adequacy decision be challenged before the Court, it is possible that the Court would reappraise the adequacy of the UK's provisions concerning data access and use for law enforcement and national security purposes.

In light of this assessment, we shall now consider what mitigation measures might be put in place should the UK lose its adequacy status.

5 Mitigation Measures

Adequacy is not the only, or even the primary, mechanism to facilitate data transfers between the EU and non-EU States. Nevertheless, it offers obvious benefits over other transfer mechanisms: namely, adequacy facilitates the seamless transfer of data by eliminating all transaction costs on data controllers and providing them with more legal certainty than other mechanisms. In interviews, participants described alternative to adequacy as messy, challenging, time-consuming and resource-intensive. It is however to these alternatives that we will now turn.

As a preliminary note, it follows from the Schrems jurisprudence that as all mitigation measures are held to the standard of essential equivalence[324], such mitigations may be of limited utility where it is impossible, or extremely difficult, for the data controller to take measures to address the deficiencies in the third-country law. Therefore, it

[322] Chris Pounder, 'Problems! Problems! Reflections on the DPDI No 2 Bill', presentation available at: <https://amberhawk.typepad.com>.
[323] Erdos, 'Towards Effective Supervisory Oversight?' (n 276) 25.
[324] *Schrems* (n 83) para 92 which confirms that the level of protection must be in place 'irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.'

would only be possible to identify definitive mitigation measures to compensate for a loss of adequacy once the reasons why the UK was deemed inadequate were known.

With this caveat in mind, we present a selection of tested mitigations and alternative approaches. Regarding tested mitigations, we present the potential for (a) a bespoke or partial adequacy agreement to be adopted, (b) the use of standard contractual clauses(c) the use of binding corporate rules, (d) public sector agreements and (e) reliance on derogations for specific situations. Regarding untested mitigations, we present (a) the definition of a transfer and (b) CoC and certification.

5.1 Tested Mitigation Measures

First, we present tested mitigations which might facilitate data transfers to NI if the existing UK adequacy decisions are invalidated or repealed, and which are based on solutions already in use in other geographic areas or use cases.

(i) Bespoke or Partial Adequacy Agreement

If the existing UK adequacy decision is no longer suitable (because of repeal, invalidation or otherwise), a modified adequacy decision is legally possible, though subject to political agreement.

The existing UK adequacy decision already expressly provides for its potential for amendment/restriction. The UK GDPR adequacy decision provides for the partial or complete suspension or repeal of the adequacy decision at the time the sunset clause elapses if 'the competent United Kingdom authorities fail to take those measures or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection'.[325] The Commission is also permitted, as an alternative, to amend the adequacy decision, 'in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.'[326] Thus, where

[325] Commission Implementing Decision 2021/1772/EU (n 113) recital 285.
[326] Commission Implementing Decision 2021/1772/EU (n 113) recital 2860.

politically possible, if there is a material change in UK data protection or surveillance law, we might expect first an amendment or modification of the adequacy decisions could be pursued.

To get a better sense of the types of tailoring that might be feasible, it is worth recalling some of the key differences seen in existing adequacy decisions. The Commission acknowledges that lesser types of adequacy decisions, which it labels 'partial' adequacy decisions, are possible.[327] We might identify three types of possible partial adequacy decisions, based on existing approaches.

First, adequacy decisions are commonly adopted with exclusions. There can be exclusions as to recipients, for example, the Canadian adequacy decision only covers recipients which are subject to the Canadian federal data protection law.[328] There can be exclusions as to the type of data covered, for example Israeli adequacy decision only covers data subject to automated processing,[329] the Japanese adequacy decision excludes data used for broadcasting, journalism, university, religious and pollical use,[330] and the Korean decision excludes data use for certain religious and political use and for the processing of credit information.[331] Moreover, we recall that the UK adequacy decisions exclude data transferred for immigration control purposes.[332] However, based on the potential objections to adequacy identified above, it is difficult to envisage how limiting adequacy to certain sectors or types of data would address these concerns.

Second, some territorial adequacy decisions are premised upon additional rules or frameworks being adopted. Thus the Japanese adequacy decision is based on the adoption of a set of Supplementary Rules (a type of delegated legislation) to which

---

[327] Communication from the Commission to the European Parliament and the Council, 'Exchanging and Protecting Personal Data in a Globalised World' COM [2017] 7 final, 4.
[328] Commission Decision 2002/2/EC.
[329] Commission Decision 2011/61/EU.
[330] Commission Implementing Decision 2019/219/EU.
[331] Commission Implementing Decision 2022/254/EU.
[332] Commission Implementing Decision 2021/1772/EU; Commission Implementing Decision 2021/1773/EU.

data recipients must adhere.[333] The US adequacy decisions have all been based on a self-certification scheme, where data recipients must sign up to and adhere to a set of protective principles.[334] These US decisions have been subject to challenge in the *Schrems* cases, which over time have become more extensive given the challenges associated with oversight, individual redress and governmental access to data. It is difficult to envisage how data recipients could remedy deficiencies in regulator independence and complaint-handling, if these were to cause a lack of adequacy. However, data recipients could commit to supplementary measures concerning the onward transfer of data (limiting such onward transfers to only entities falling under an existing EU adequacy decision, for instance) or introducing additional safeguards for individuals around the handling of data subject requests.

Third, there is the potential for adequacy decisions to be adopted on a partial geographic basis, addressing only a territory within a given country.[335] A favourable adequacy opinion was adopted in respect of Quebec in Canada,[336] though it did not ultimately lead to an adequacy decision, and to date, no regional adequacy decisions have been adopted. Nevertheless, it remains a possibility that a bespoke adequacy decision for NI could be pursued. Negotiating such a bespoke arrangement may be politically contentious as it would likely entail a prohibition or limitation of onward data transfers from NI to the UK. This could be framed as a necessary corollary to NI's regulatory alignment with the EU under the Windsor Framework. However, it could equally lead to concerns about the creation of a digital border in the Irish sea. Moreover, those entities that are reliant on the free flow of data between both the rest of the UK and the EEA would face the daunting practical task of navigating dual regulatory environments. Beyond its political feasibility, depending on the adequacy 'fault' identified, it may be difficult to disentangle the legal framework to ensure that NI

[333] Commission Implementing Decision 2019/219/EU.
[334] Commission Decision 2000/520/EC; Commission Implementing Decision 2016/125/EU; Commission Implementing Decision 2023/4745/EU.
[335] Article 45(1) GDPR.
[336] A29WP, 'Opinion 7/2014 on the protection of personal data in Quebec', adopted on 4 June 2014, WP 219.

avoids this fault. For example, if the issue is with the independence of the regulator, then it is the same regulator that ensures oversight across the UK. Addressing this deficiency would require the establishment of independent oversight of data processing in NI. While this is not impossible, and the ICO already has an office in Belfast, it would again require political support and any issues concerning it compatibility with the devolution settlement for NI would need to be assessed. Moreover, the challenges associated with onward transfers outside of NI but within the UK would persist. Given the practical, administrative, and potential political implications, any appetite for such an approach seems implausible.

(ii) Standard Contractual Clauses

Standard Contractual Clauses (or 'SCCs') are a type of 'appropriate safeguard' which can legitimate data transfers under Article 46. The logic of the SCCs is that the continuity of data protection standards can be ensured through a contractual agreement to uphold certain data protection guarantees. These are, in essence, model contracts which have been adopted by the Commission and which may be used by data exporters to legitimate the data transfer. Several versions of SCCs have been adopted over the years, but the latest version is found within Commission Implementing Decision 2021/914/EU, which was adopted after *Schrems II*.[337]

SCCs can be used for a broad set of scenarios: they can be used for transfers by either a data controller or data processor, to a processor or controller established in a 3rd country and they may be used by natural or legal persons, public authorities, agencies or other bodies.[338]

The SCCs, as model contracts, contain a set of clauses which can be adopted and adapted by exporters and importers. They take a modular approach, which means that the parties select the applicable elements (i.e. clauses) for their circumstances. They

[337] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. L 199/31.
[338] Cl 1(b), Annex to Commission Implementing Decision (EU) 2021/914.

can be integrated into broader contracts, provided other clauses of that agreement do not conflict with the SCCs.[339] The parties to the SCCs must describe the details of the transfer, the categories of personal data transferred and the purposes of transfer.[340]

The nature of the protections are set out in detail, as each party must make a series of binding promises as to their respective obligations. The exporter warrants that it has used 'reasonable efforts' to determine the importer is able to implement a series of protections.[341] Those protections are determined according to the type of relationship – whether transfer from a controller to a controller, from a controller to a processor, from a processor to a processor, or from a processor to a controller. For each of these relationship types a 'Module' of clauses to be incorporated is provided. The most extensive protections are found in the controller-to-controller module.[342] The other relationships contain variations or components of these requirements. Where the importer is receiving the data as a data processor, clauses as to the use of sub-processors must also be included.[343]

Protections are put in place for data subjects. In all cases, clauses on data subject rights must be included.[344] Further, data subjects may enforce certain clauses of the SCCs as third party beneficiaries.[345] Additionally, clauses which provide for data subject redress must be included, including an agreement by the importer to abide by a decision that is binding under EU or Member State law.[346] A liability clause must be included, which provides for a right to compensation to the data subject among other provisions.[347] Both the data exporter and importer must agree to be regulated by a

---

[339] Cl 2(b), Annex to Commission Implementing Decision (EU) 2021/914.
[340] Cl 6, Annex to Commission Implementing Decision (EU) 2021/914.
[341] Cl 8, Annex to Commission Implementing Decision (EU) 2021/914.
[342] These include guarantees as to purpose limitation, transparency, accuracy and data minimisation, storage limitation, security of processing, processing of sensitive data, onward transfers, processing under the authority of the data importer and documentation and compliance. Module 1, Clause 8, Annex to Commission Implementing Decision (EU) 2021/914.
[343] Cl 9, Annex to Commission Implementing Decision (EU) 2021/914.
[344] Cl 10, Annex to Commission Implementing Decision (EU) 2021/914.
[345] Cl 3(a), Annex to Commission Implementing Decision (EU) 2021/914.
[346] Cl 11, Annex to Commission Implementing Decision (EU) 2021/914.
[347] Cl 12, Annex to Commission Implementing Decision (EU) 2021/914.

national supervisory authority of a Member State.[348] The parties must choose a governing law, which must be the law of one of the EU Member State,[349] and choose a forum and jurisdiction (again, ordinarily of an EU Member State.[350]

The parties must warrant they have no reason to believe local laws and practices will affect compliance with the SCCs,[351] and clauses are put in place to deal with obligations of the data importer when there is access by public authorities.[352] Additionally, a clause dealing with non-compliance and termination of the SCCs must be included.[353]

The SCCs are a satisfactory solution for many organisations, particularly those which have the resources to put them in place, and where relationships are ongoing such that the investment in terms of legal and organisational budget is worthwhile. As the most commonly used transfer mechanism, the SCCs are a comparatively well-tested mechanism and those wishing to use the SCCs have the expertise of others with experience in their application to learn from. Indeed, global companies operating in NI may already have experience with their application in some instances. This was noted in several interviews. The Department for Agriculture, Environment and Rural Affairs (DAERA) had worked with existing partners to draw up and sign SCCs covering data flows pertaining to areas such as veterinary services.[354]

At the same time, there is a business cost to putting SCCs in place, to ensure they are legally sound and in terms of ongoing monitoring and compliance cost. Although it is the data exporter who puts the SCC in place, it requires the input and ongoing cooperation of the data importer. The Department for Communities, the biggest department in the NI civil service with a wide-reaching remit ranging from benefits to sporting provision, had envisaged the use of SCCs with partner organisations in the

[348] Cl 13, Annex to Commission Implementing Decision (EU) 2021/914.
[349] Cl 17, Annex to Commission Implementing Decision (EU) 2021/914.
[350] Cl 18, Annex to Commission Implementing Decision (EU) 2021/914.
[351] Cl 14, Annex to Commission Implementing Decision (EU) 2021/914.
[352] Cl 15, Annex to Commission Implementing Decision (EU) 2021/914.
[353] Cl 16, Annex to Commission Implementing Decision (EU) 2021/914.
[354] Interview, Philip Gilmore, Head of Data Protection and Information Management, DAERA.

RoI in the absence of adequacy. It was noted however that the Department's small information governance team might struggle to handle the additional workload leading to a detrimental impact on operations by slowing everything down.[355]

Furthermore, in contrast to adequacy decisions, because SCCs can be adopted notionally for any country of destination, in line with the *Schrems II* decision, the data exporters are also obliged to conduct a transfer impact assessment, in order to assess whether there are any reasons why the SCCs are not suitable. Accordingly, there may be some jurisdictions where the SCCs are not deemed suitable, because of legal or other features of the destination country.[356] If an entity based in NI and the RoI respectively agreed to facilitate an EU-UK data transfer between them through the SCCs, they would be required to warrant that they had 'no reason to believe that the laws and practices' of the UK, 'including any requirements to disclose personal data or measures authorising access by public authorities' would prevent the Northern Irish entity from fulfilling its obligations under the SCC.[357] Thus, again, depending on the reason for the refusal to recognise the UK as adequate or the invalidity of an adequacy decision, it may be difficult for the data exporter and importer to provide such legal guarantees. The existence of any UK laws and practices that could cause disproportionate interference with fundamental rights applicable to the personal data imported by the Northern Irish entity would be problematic under this clause.[358] In providing their warranty, both the Northern Irish and Irish entities would be declaring that they had taken due account of a number of factors, including: the specific circumstances of the transfer; UK laws and practices; and any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards provided in the SCC.[359] The EDPB and EDPS emphasise that even where the new

[355] Interview, Karen McMullan, Head of Information Management, Department for Communities.
[356] See Recitals 18, 19 and 22, Commission Implementing Decision (EU) 2021/914.
[357] Cl 14(a) Annex to Commission Implementing Decision (EU) 2021/914.
[358] Assessed on the basis of whether the law or practice is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR. Among this long list of legitimate purposes are the protection of national security; the prevention, investigation, and prosecution of crime; and the enforcement of civil claims.
[359] Cl 14(b) Annex to Commission Implementing Decision (EU) 2021/914.

SCCs are used, ad-hoc supplementary measures may still be necessary in some circumstances to ensure that data subjects receive an essentially equivalent level of protection. The need to conduct this impact assessment also adds to the compliance cost associated with SCCs. Accordingly, SCCs may prove too costly for small scale data transfers. For instance, researchers benefitting from small pots of seed funding to get research projects up and running (such as those funded by SCoTENS alluded to above) might no longer have the institutional support required to put such arrangements in place for small sums of money.

(iii) Binding Corporate Rules

Binding Corporate Rules (BCRs) are another type of 'appropriate safeguard' which can legitimate data transfers under Article 46 GDPR and which are provided for in Article 47 GDPR. BCRs are a set of legally binding rules to which members of a group of undertakings (e.g. a corporate group) sign up, promising to apply certain protective standards to intra-group data transfers. These BCRs must be approved by a data protection authority before they are valid, and the GDPR sets out a lengthy list of factors which must be reflected in the BCRs.[360]

By their very nature, BCRs are suitable for a narrower set of transfers than adequacy decisions or SCCs; namely, intra-organisational transfers. They are thus particularly useful for large multi-national organisations which have multiple corporate forms within that group. In such cases, where SCCs are no longer practical because of the number of entities or data transfers being conducted, BCRs are another option to achieve compliance. BCRs can be used to transfer data originating from a controller, or from a processor.

The process for BCR approval is relatively complex, particularly given the cross-border cooperation between data protection authorities which is often engaged. First, the applicant must complete the standard form for application (either the controller or processor form), and submit it to a single data protection authority, who acts as the

[360] Article 47 GDPR.

lead (coordinating authority) for the purposes of the approval. The approval process is then subject to the consistency mechanism set out in Article 63 GDPR, before the BCRs can be approved.

A series of elements which must be contained in the BCRs is set out in Article 47(2) GDPR and then supplemented with guidance by the EDPB.[361] BCRs will require, amongst other things, an employee training process, a network of data protection officers or appropriate staff, a complaint handling process, and an audit program.

BCRs come with a considerable business/compliance cost, in part associated with the lengthy and complex approval process, but also due to the need to implement a comprehensive data protection organisational program. An additional complication is that, as yet, there is no harmonised approach for UK and EU BCRs, and consequently, reconciling a BCR programme which satisfies the UK GDPR and the ICO with an EU BCR programme is not easily achieved. Additionally, as with SCCs, BCRs cannot overcome problems of the wider legal regime (e.g. governmental data access), and commitments with regards to governmental access requests must now be built into BCR applications.[362]

(iv) International Agreements Between Public Authorities or Bodies

Third-country public authorities or bodies have an additional option available to them when seeking to identify a mechanism that could facilitate transfers from an EEA public authority or body. In the absence of an adequacy decision, an EEA public authority or body may meet the requirement of providing appropriate safeguards for the transfer of personal data through 'a legally binding and enforceable instrument' with a third-country public authority or body.[363] The EDPB specify that 'international treaties, public-law treaties or self-executing administrative agreements' may be used for this

[361] The most recent guidance is found in EDPB, 'Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)', adopted on 20 June 2023 (v 2.1).
[362] ibid.
[363] Article 46(2)(a) GDPR.

purpose.[364] This may be done on a bilateral or multilateral basis.[365] The EDPB provides access to administrative arrangement on its website.[366]

Where appropriate safeguards are provided for through a non-binding administrative arrangement (for example, with the drafting of a non-binding memorandum of understanding), authorisation from the competent supervisory authority must also be obtained.[367] Authorities should only choose to rely on non-legally binding administrative arrangements after careful consideration. If a non-binding agreement is relied upon by an EEA public authority engaging with a NI public authority, specific assurances should be provided by the NI public authority regarding the protection of individual rights in Northern Irish law and the accessibility of remedies for EEA individuals in NI.[368]

The EDPB provides general recommendations for what an international transfer agreement between public bodies should contain in order to be GDPR compliant.[369] The minimum safeguards elaborated by the EDPB are designed to ensure that EEA data subjects retain an equivalent level of protection when their data is transferred outside of the EEA.

The agreement should clearly define its purpose and scope and state the categories of data affected and the type of processing covered. Definitions must be provided for the basic concepts of data protection law in line with the GDPR. Specific wording should be included guaranteeing protection of the data protection principles by both parties. Details should be provided regarding how those principles will be followed in

---

[364] EDPB, 'Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and Non-EEA Public Authorities and Bodies' v2.0, adopted on 15 December 2020', 17.

[365] ibid, 7.

[366] EDPB, 'Administrative arrangement', https://edpb.europa.eu/our-work-tools/our-documents/topic/administrative-arrangement_en.

[367] Article 46(3) and recital 108 GDPR.

[368] The EDPB notes that 'If this is not the case, individual rights should be guaranteed by specific commitments from the parties, combined with procedural mechanisms to ensure their effectiveness and provide redress to the individual.' EDPB 'Guidelines 2/2020' (n 364) 17-18.

[369] ibid.

practice. For example, the agreement should specify the purposes for which the data is being transferred and processed.[370] Crucially, the agreement must ensure 'enforceable and effective data subject rights' and 'the specific commitments taken by the parties to provide for such rights' in practice.[371] The Guidelines further detail how data subject rights should be specifically provided for. For example, as regards the right of access, the agreement should specify what modalities are available to data subjects seeking to exercise their rights.[372]

In their comments on the first published version of the EDPB Guidelines, the Norwegian Institute of Public Health and the Cancer Registry of Norway stated that

> Scientific researchers have struggled to identify an appropriate safeguard under the GDPR for cross-border transfer of personal data to third countries and international organizations. This has gravely affected scientific research collaborations in the health research field.[373]

The Norwegian Institute asserted that the EDPB Guidelines on public authority to public authority transfers posed an obstacle to the establishment of an administrative arrangement with US-based health authorities. For example, it was unclear whether the archiving requirements under the US Federal Records Act would be covered under the derogations for scientific research and archiving purposes in the public interest in the GDPR.[374] For these reasons, ALLEA (European Federation of Academies of Sciences and Humanities) concluded that administrative arrangements do not provide a 'viable solution to solve the challenges of international transfers, especially with

---

[370] The EDPB provide additional guidance on how the other principles should be specifically provided for in the Guidelines. ibid.
[371] ibid, 9.
[372] ibid, 10.
[373] EDPB, 'Norwegian Institute of Public Health and the Cancer Registry of Norway Comments on Proposed EDPB Guidelines 2/2020' [2020] <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_guidelines_niph_crn_comments_20200518.pdf>.
[374] ibid.

regard to US federal institutions.'[375] It is notable that the EDPB did clarify some of these issues in Version 2.0 of the Guidelines following consultation. For example, in its provision for the purpose limitation principle, it was noted that

> Compatible purposes may include storing for archiving purposes in the public interest, as well as processing for scientific or historical research purposes or statistical purposes. It is recommended, for better clarity, that the specific purposes for the processing and transferring of the data are listed in the international agreement itself.[376]

As with the other mechanisms for transfer with appropriate safeguards provided for in the GDPR, EU law places onerous requirements on the transferring public body 'to assess whether the level of protection required by EU law is respected in the third country, in order to determine whether the list of safeguards included in the international agreement can be complied with in practice, taking into account the possible interference created by the third country legislation with compliance with these safeguards.'[377]

Due to the importance of cross-border administrative collaboration, this mechanism may have some useful application for Northern Irish public authorities where they are engaging with other public bodies and not private entities.[378] The use of such a mechanism would, however, trigger some broader legal queries. Most apparently, whether a NI public authority has the competence (under the devolution settlement amongst others) to enter into international agreements is doubtful. Moreover, it is uncertain that a NI Department could waive the jurisdiction of a UK regulator (such as

---

[375] ALLEA (European Federation of Academies of Sciences and Humanities), FEAM (Federation of European Academies of Medicine), and EASAC (European Academies' Science Advisory Council), International Sharing of Personal Health Data for Research (ALLEA 2021) <https://doi.org/10.26356/IHDT>.

[376] EDPB 'Guidelines 2/2020' (n 364) 8.

[377] ibid, 7.

[378] This mechanism is not designed to cover transfers related to public security, defence or state security (see GDPR art 2(2)) or transfers for criminal law enforcement purposes (see LED). ibid, 5.

the ICO) and agree to be under the jurisdiction of an EEA regulator if issues such as complaint-handling or independent enforcement were disputed.

(v) Derogations for Specific Situations.

Article 49 GDPR allows for 'derogations for specific situations'. This sets out grounds for transfer that can apply in the absence of an adequacy agreement or appropriate safeguards. These grounds include situations where the data subject explicitly consents having been advised of the risks of such transfer following from the lack of adequacy or alternative; where the transfer is necessary for the conclusion or performance of a contract; or where the transfer is necessary for important reasons of public interest, amongst others.[379] It provides that where none of the specified derogations apply, the transfer may (still) take place but only if the transfer:

- is not repetitive;
- concerns only a limited number of data subjects;
- is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the rights or interests of the data subject
- the controller has assessed the circumstances of the transfer and has put in place suitable data protection safeguards; and,
- The controller has informed the supervisory authority and the data subjects of the transfer.

The EDPB considers the Article 49 derogations to be 'exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards'.[380] The EDPB Opinion confirms that this provision exceptionally allows transfers to third countries

[379] The full list is found in Article 49(1)(a)-(g) GDPR.
[380] EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679', adopted on 25 May 2018, 4.

where there is inadequate protection (whether through a lack of adequacy or appropriate safeguards).[381]

The non-binding recitals of the GDPR, which guide its interpretation, state that some of the derogations found in Article 49(1) (those relating to contract and legal claims[382]) are limited to 'occasional transfers'. The EDPB nevertheless considers that the other derogations (including explicit consent and important reasons of public interest) should be interpreted in a way that does not contradict their very nature as derogations which should be interpreted restrictively.[383] In *Schrems II*, the Court held that the annulment of the Privacy Shield would not create a legal vacuum as the derogations in Article 49 could be relied upon. This seems to suggest that the Court is willing to allow these derogations to be used even in cases of regular data transfers between the EU and inadequate third countries.[384]

This begs the question of how the Article 49 derogations might be used in the NI context. For instance, it seems possible that for cross-border workers living in the RoI but working in NI that they could give explicit consent to have their personal data processed for payroll or pension purposes, or that suppliers of goods or services to EU customers might process certain data which is necessary for the fulfilment of a sales contract. What remains less clear is whether this solution could be used at scale, for instance if a factory in NI employed a lot of individuals living in the RoI. The EDPB might consider that this would turn the exception into a rule while the Court's statement in Schrems II seems to suggest this would be a viable option. The disadvantage of this

---

[381] It states that: 'Data exporters should therefore favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data once this data has been transferred. As derogations do not provide adequate protection or appropriate safeguards for the personal data transferred and as transfers based on a derogation are not required to have any kind of prior authorisation from the supervisory authorities, transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned.' ibid.
[382] Article 49 (1)(b)(c) and (e) GDPR.
[383] EDPB, 'Guidelines 2/2018' (n 380) 5.
[384] *Schrems II* (n 95) para 202.

option is the extra administrative work required in order to obtain explicit and valid consent meeting GDPR requirements.

5.2 Untested Mitigation Measures

Other lesser known or untested mitigation measures might also be relevant. These include (i) narrowing the definition of what constitutes a transfer to avoid the application of the GDPR transfer rules; (ii) CoC; (iii) certification mechanisms; and, most speculatively, (iv) international trade challenges.

(i) The Limited Definition of a Data Transfer

The GDPR does not expressly define the concept of 'data transfer' under Chapter V. This fact, combined with the extra-territorial rules of the GDPR, and the lack of any coordination between these elements of the GDPR, creates some disagreement as to the precise definition of a transfer. Thus, a relatively high-risk option is for data exporters to argue that certain processing operations, where the recipient is subject to the GDPR by virtue of its extra-territorial rules, are not data transfers within the meaning of Chapter V of the GDPR.

The GDPR, through Article 3, has extra-territorial application, and thus some entities outside the EEA may be subject to its obligations. The GDPR applies to processing of personal data "*in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*"[385] Equivalent language in the Data Protection Directive has been interpreted by the ECJ very broadly, such that entities not based in the EU with subsidiaries or other stable arrangements in the EU were captured by EU law.[386] Further, the GDPR applies to entities based outside the EU who process data associated with offering goods or services to data subjects in the EU or are monitoring the behaviour of data

[385] Article 3(1) GDPR.

[386] See, for instance, Google Spain (n 81) and Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388. See, more generally, Merlin Gömann: 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) Common Market Law Review 567.

subjects in the EU.[387] Finally, the GDPR also applies to processing in a place where Member State law applies by virtue of public international law (e.g. in embassies).[388]

Thus the question arises, if data is being provided to an entity which is already subject to the GDPR by virtue of these extra-territorial rules, but which is not in the EU, is this a data transfer? There is a disagreement between the EDPB guidelines and the Commission's apparent position, which creates the scope for making an argument that no transfer is occurring.

The EDPB has adopted guidelines which sets out its position as to when a data transfer occurs.[389] These guidelines provides that three criteria must be satisfied for a transfer to occur:

> *1) A controller or a processor ("exporter") is subject to the GDPR for the given processing.*
>
> *2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").*
>
> *3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.*[390]

Thus, the EDPB's position is that the importer's location in a third country is determinative, rather than whether it is already subject to the GDPR via the GDPR's extra-territorial rules. It justifies this by pointing to the purpose underlying the data transfers rule (to prevent data protection being undermined), and argues that even if the processing is subject to the GDPR, the importer could nevertheless be 'subject to

---

[387] Article 3(2) GDPR.
[388] Article 3(3) GDPR.
[389] EDPB, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR', v.2.0, adopted on 14 February 2021.
[390] ibid, para 9.

different (conflicting) legal frameworks, e.g. as regards possible disproportionate government access to personal data.'[391] As Kuner has argued, "the GDPR cannot operate outside the EU exactly as it does within it, since it is based on the EU's legal framework in areas such as the recognition and enforcement of judgments, the rule of law, the independence of the judiciary and the DPAs, and other fundamental rules that by their nature are not addressed to third countries."[392] Thus the EDPB's position is grounded in a protective rationale, which reflects the purposive approach which is characteristic of the EDPB, and often of the CJEU.[393]

However, the Commission appears to have taken a different position, at least in some instances. In the latest SCC Decision, Recital 7 is illuminating:

> *A controller or processor may use the standard contractual clauses set out in the Annex to this Decision to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof), because it relates to the offering of goods or services to data subjects*

[391] ibid, para 23.

[392] Christopher Kuner, 'Protecting EU data outside EU borders under the GDPR' [2023] 60(1) Common Market Law Review 77, 86.

[393] Under the Data Protection Directive, in *Lindqvist* (Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971), the Court found that 'In order to determine whether loading personal data onto an internet page constitutes a transfer of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country, it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV of that directive where Article 25 appears.', para 57.

> *in the Union or the monitoring of their behaviour as far as it takes place within the Union.*[394]

The Commission therefore appears to suggest that if the importer is subject to the GDPR, no data transfer has occurred.

Similar language appeared in the Privacy Shield adequacy decision:

> …The Principles apply solely to the processing of personal data by the U.S. organisation in as far as processing by such organisations does not fall within the scope of Union legislation. The Privacy Shield does not affect the application of Union legislation governing the processing of personal data in the Member States.[395]

Moreover, Kuner reports that 'the Commission has indicated that it is likely to insert language in adequacy decisions mirroring that used in the SCCs, i.e. indications that an adequacy decision does not apply to transfers to a data importer whose processing of the data is directly subject to the GDPR.'[396]

Nevertheless, this is a higher risk strategy to adopt. This difference between the EDPB and the Commission reflects an uncertainty as to the definition of a transfer, and the CJEUs historic rights-protective stance suggests that it may well find in favour of the EDPB approach, should the question come before the CJEU.

A further way in which the definition of what constitutes a transfer might be relevant concerns transfers within the same organisational structure. The EDPB states that Chapter V does not apply to 'internal processing' which it defines as 'where data is not disclosed by transmission or otherwise made available to another controller or processor, including where such processing takes place outside the EU'. The rationale is that in this case, the EU-based controller or processor remains responsible for GDPR

---

[394] Commission Implementing Decision (EU) 2021/914, Recital 7 (emphasis added).
[395] Commission Implementing Decision 2016/125/EU, recital 15.
[396] Kuner, 'Protecting EU data outside EU borders' (n 392) 93.

compliance.[397] This begs the question, from a corporate governance perspective, of when entities are considered to be the same entity even though their operations straddle different jurisdictions. Some of the examples used by the EDPB may provide additional insights: the EDPB considers that when a subsidiary controller in the EU shares employee data with its parent company (a processor) in a third country there is a transfer.[398] The reason why this does not constitute 'internal processing' is not apparent. The EDPB notes that where an EU employee accesses data remotely in a third country there is no transfer as the employee is not another controller; the transmission is carried out within the same controller.[399] It remains at least ambiguous on the basis of these observations whether an entity which has an establishment north and south of the border in Ireland could claim that transfers from the RoI to NI (for instance, of employee data) are 'internal processing' and do not fall within the scope of Chapter V. One entity that we interviewed had received advice to this effect prior to the adoption of the UK adequacy decision.

(ii) Codes of Conduct

Codes of Conduct (CoC) are a tool provided by the GDPR with the potential to help facilitate international data flows.[400] They have been described as 'complementary tools to the GDPR that can offer additional legal certainty to specific sectors or actors engaged in specific processing activities.'[401] Others have highlighted the potential utility of CoC for SMEs 'searching to do the right thing and sustain consumer trust'[402] and the potential of such codes to provide both SMEs and micro businesses with a

---

[397] EDPB, 'Guidelines 5/2021' (n 389) para 18.
[398] ibid, 22.
[399] ibid, 21.
[400] European Commission, 'Communication: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' [2020] 11–12.
[401] Carl Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features: A Tale of Two Systems' [2022] 12 International Data Privacy Law 297, 300.
[402] Jennifer Baker, 'Will the GDPR Incite Sectoral CoC?' (IAPP, 19 December 2018) <https://iapp.org/news/a/will-the-gdpr-incite-sectoral-codes-of-conduct/>.

more cost effective mechanism for data protection compliance.[403] In light of this, it is particularly important to consider their potential application in the Northern Irish context.

Article 40 provides that bodies representing categories of controllers or processors – including trade, representative, academic organisations and interest groups[404] – may develop CoC 'for the purpose of specifying the application' of the GDPR.[405] CoC should help to 'support compliance with data protection issues identified or specific' to the relevant sector. Once a code of conduct is approved, relevant entities will be able to sign up to the code 'to enhance and demonstrate their compliance with data protection legislation'.[406]

Adherence to a code of conduct may fulfil the need for the 'appropriate safeguards' required by the GDPR when data is transferred to a third country without an adequacy decision.[407] CoC are comparatively under-explored in the academic literature, but the EDPB has published official transnational codes and guidelines for the use of CoC as tools for transfers.[408] Among the non-exhaustive list of examples provided in Article 40 GDPR of matters that could be addressed in CoC is the 'transfer of personal data to third countries or international organisations'.[409] Where a code is intended for transfers

---

[403] EDPB, 'Guidelines 1/2019 on CoC and Monitoring Bodies under Regulation 2016/679' [2019] 8 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf> .

[404] ibid 11.

[405] Article 40(2)(j) GDPR.

[406] Data Protection Commission, 'What Are CoC?' <https://www.dataprotection.ie/organisations/codes-conduct>.

[407] Art 46(1)(e) GDPR. According to Article 46 GDPR, the appropriate safeguards may be provided for by 'an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights'. See also Article 40(3) GDPR.

[408] The EDPB website lists seven approved – national and transnational – CoC. CoC, amendments and extensions See for example: 'Data Protection Code of Conduct for Cloud Infrastructure Service Providers, 9 February 2021' <https://edpb.europa.eu/system/files/2023-03/2021_cispe_cloud_iaas_data_protection_code_of_conduct_-_gdpr_compliance_0.pdf>. EDPB, 'Guidelines 04/2021 on CoC as tools for Transfers', adopted on 22 February 2022; EDPB, 'Guidelines 1/2019' (n 403); Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features' (n 401) 298.

[409] Article 40(2)(j) GDPR.

and for the purpose of providing 'appropriate safeguards', the code should not only address the 'essential principles, rights and obligations' of the GDPR, but must also address the 'the guarantees that are specific to the context of transfers'.[410] The EDPB provides a checklist of elements to be covered by a code of conduct intended for transfers. Among this list of elements to be included are provision for data subject rights as provided for by the GDPR (including the right of access), provision for data subject rights to enforce the code as third-party beneficiaries, and provision of an appropriate complaint mechanism.[411]

The GDPR provides for three different categories of code that apply in situations of different territorial reach.[412] These three categories have been labelled as 'national codes',[413] 'transnational codes'[414]; and 'codes having general validity'.[415] In order to be operative, national codes must be approved by a competent supervisory authority[416] while transnational codes follow a more elaborate approval process involving affected Member States and the EDPB. [417] To be approved as a 'code having general validity', the EU Commission must decide that the approved transnational code of conduct has 'general validity within the Union.'[418] Codes deemed to be of general validity can apply to all Member States. As noted by Vander Maelen, being approved

[410] EDPB, 'Guidelines 04/2021' (n 408) 3.
[411] ibid 13.
[412] Article 40(5)-(9) GDPR.
[413] Article 40(5) and 40(6) GDPR. National codes can be applied to 'processing activities contained in one Member State'
[414] Article 40(7) GDPR. 'Transnational codes' can apply to 'processing activities in several Member States'
[415] Article 40(9) GDPR; Article 40(7) GDPR; Vander Maelen 'GDPR CoC and Their (Extra)Territorial Features' (n 401) 305.
[416] Article 40(6) GDPR.
[417] Transnational codes must be approved by the supervisory authority of the code's country of origin following the review of the draft code by the supervisory authorities of the other affected Member States and the provision of an opinion by EDPB on whether the draft code complies with the GDPR or provides appropriate safeguards : Article 40(7) GDPR.
[418] Article 40(8)-(9) GDPR.

as having general validity is likely to 'attract new actors to a code who may not previously have been interested'.[419]

While the EDPB maintains that '[o]nly those codes having been granted general validity within the Union may be relied upon for framing transfers',[420] depending on the EU 'establishment' status and scope of operations of a third country entity, they may be able to utilise the other categories of code in their compliance efforts. Many Northern Irish entities fall within the territorial scope of the GDPR which is defined broadly in Article 3 GDPR. For example, Northern Irish entities with an 'establishment' in the EU fall within the scope of the Regulation, regardless of where the processing takes place.[421] Moreover, the related activities of Northern Irish entities monitoring or offering goods or services to EU-based data subjects also fall within the territorial scope of the GDPR.[422] Such entities may consider utilising national, transnational, or codes of 'general validity' to facilitate their operations.[423]

If the entity's activities cannot be considered to fall within the scope of Article 3 of the GDPR, there is still the potential to utilise codes. Notably, Article 40 provides that controllers or processors that are not subject to the GDPR may adhere only to CoC that are deemed to have 'general validity' and that have been approved by a competent supervisory authority.[424] The requirement for codes to be of 'general validity' in this context is likely due to the role of the Commission in approving those codes.[425] Article 40(3) GDPR explicitly states that the purpose of codes in this context is to ensure the provision of 'appropriate safeguards within the framework of personal data transfers to third countries' or international organisations. As part of this, such controllers or processors are required to 'make binding and enforceable commitments, via

---

[419] Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features' (n 401) 309.
[420] EDPB, 'Guidelines 04/2021' (n 408) 10.
[421] Article 3(1) GDPR.
[422] ibid, Article 3(2).
[423] Note that the EDPB distinguishes between code members located in the EEA and code members located outside the EEA due to the 'the direct application of the GDPR to the former but not the latter (provided that the latter does not fall under Article 3.2 GDPR)'. EDPB, 'Guidelines 04/2021' (n 408) 11.
[424] Article 40(3) GDPR.
[425] Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features' (n 401).

contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.'[426]

For example, a Northern Irish entity with an establishment in RoI (or another EU Member State) may be able to transfer data originating from RoI to other Northern Irish entities that are not subject to the GDPR if the data recipient adheres to a code of general validity.[427] In this instance, the Irish entity transferring the originating data would not need to adhere to the code of conduct themselves but could rely on the importer's adherence to the code for the purposes of third country transfer.[428]

As elaborated by the EDPB, CoC intended for transfers could be developed by bodies representing a sector or by separate sectors with a 'common processing activity'. For example, the EDPB provides the example of a human resources code which could be drawn up by an association of HR professionals. Such a code could facilitate multiple transfers to a separate entity that is located in a third country without adequacy status.[429]

Considering the significant healthcare and research cooperation between NI and RoI, there is a potential use case for a code of conduct to be developed by health sector representatives.[430] For example, as suggested by the EDPB,

---

[426] Article 40(3) GDPR.

[427] For general examples, Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features' (n 401) 309-310.

[428] EDPB, 'Guidelines 04/2021' (n 408) 3.

[429] ibid 6.

[430] Demonstrating interest in the mechanism of CoC in the sector, in 2022, the Spanish supervisory authority approved an industry code of conduct 'to enable compliance of clinical research and pharmacovigilance with the GDPR'. Interestingly, significant yet unsuccessful efforts were made under the framework provided by the Data Protection Directive to establish a Code of Conduct on privacy for mHealth apps. <https://www.aepd.es/es/pre nsa-y-comunicacion/notas-de-prensa/aepd-aprueba-primer-codigo-con ducta-sectorial-desde-entrada-vigor-rgpd>. <https://www.aepd.es/es/pre nsa-y-comunicacion/notas-de-prensa/aepd-aprueba-primer-codigo-con ducta-sectorial-desde-entrada-vigor-rgpd> European Commission, Privacy code of conduct on mobile health apps <https://digital-

> An association representing categories of controllers/processors involved in the same type of research activities for the health sector and involving regular transfers of data to third country controllers/processors develop a code of conduct which is also intended to be used as a tool for transfers. Relevant controllers/processors in the EEA adhere to this code of conduct which is also being adhered to by third country controllers/processors. The transfers of data to third country controllers/processors as part of the research activities can be framed with this code of conduct.[431]

In light of the above, CoC may be of utility in the context of data transfers for some sectors and certain actors located in NI in the event of a loss of adequacy. It should be noted, however, that drafting and having codes approved is a significant undertaking, requiring an investment of resources by the 'code owner' and interaction and approval from a national supervisory authority in all cases, an opinion from the EDPB in the case of transnational codes, and further Commission approval in the form of an implementing act in the case of codes of 'general validity' – likely to be desirable in a post-adequacy environment. Moreover, a feature of codes of conduct applicable to private actors is the delegation of certain supervisory functions to 'monitoring bodies' with 'an appropriate level of expertise in relation to the subject-matter of the code'. These bodies must be 'accredited for that purpose by the competent supervisory authority'.[432] The limited number of such codes in operation is indicative of the extent of the task in practice. In addition to the requirement for approval by the Commission, codes of general validity may also be considered to suffer from an additional incentive challenge. Maelen has noted that the 'incentive for actors who are already subject to the GDPR (…) to invest resources in developing a code that goes even further than a

---

strategy.ec.europa.eu/en/policies/privacy-mobile-health- apps> 82. Elisabeth Steindl, 'Safeguarding Privacy and Efficacy in E-Mental Health: Policy Options in the EU and Australia' [2023] International Data Privacy Law ipad009, 12.

[431] EDPB, 'Guidelines 04/2021' (n 408) 7.

[432] Article 41(1) GDPR. Article 41(6) GDPR states that 'This Article shall not apply to processing carried out by public authorities and bodies'.

transnational code is not clear.'[433] Yet, such codes would be of clear use to actors not subject to the GDPR but who need to receive data from the EU.[434] In spite of these issues, it is plausible that sufficient motivation will exist to pursue the development of CoC in certain contexts due to the important ties across many sectors in NI and RoI.

(iii) Certification

Another tool of co-regulation with some common features with CoC are certification schemes.[435] The third-party certification schemes provided for in the GDPR should help controllers and processers to achieve and demonstrate compliance with the GDPR. Like with CoC, the provisions on certification make specific reference to the needs of micro, small and medium-sized enterprises.[436] Article 42 GDPR states that the establishment of 'data protection certification mechanisms and of data protection seals and marks' should be encouraged. Recital 100 GDPR suggests that the aims of this policy are 'to enhance transparency and compliance' and to allow data subjects to 'quickly assess the level of data protection of relevant products and services.'[437]

Article 46(2)(f) GDPR makes clear that an approved certification mechanism can provide the 'appropriate safeguards' necessary for third country data transfer. It is notable that Article 42(2) GDPR provides for the use of certification mechanisms by controllers and processors that are not subject to the GDPR where such parties 'make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.'.[438] A 'selling point' of certification is that it gives entities not subject

[433] Vander Maelen, 'GDPR CoC and Their (Extra)Territorial Features' (n 401) 309
[434] ibid.
[435] EDPB, 'Opinion 28/2022 on the Europrivacy Criteria of Certification Regarding Their Approval by the Board as European Data Protection Seal Pursuant to Article 42.5 (GDPR)', adopted on 10 October 2022.
[436] ibid, Article 42(1).
[437] ibid, recital 100.
[438] ibid, Article 42(2).

to the GDPR the opportunity to conform to its principles when importing GDPR-protected data .[439]

Where the certification of a third-country data importer is relied upon as an appropriate safeguard under the GDPR, the controller exporting the data must confirm that the relevant certification will be effective. This requires verification that the relevant certificate is valid and whether 'it covers the specific transfer to be carried out and whether the transit of personal data is in the scope of certification'.[440] As noted by the EDPB, the exporter is also obliged to consider whether the certification 'is effective in the light of the law and practices in force in the third country that are relevant for the transfer at stake'.[441] The EDPB has specified that certification mechanisms as tools for transfers must include additional elements in order to ensure consistency with other transfer mechanisms and in order to address the findings in *Schrems II*.[442]

Theoretically, third-party certification could be a valuable tool in a post-adequacy environment.[443] If an appropriate scheme for certification was identified, a Northern Irish entity could seek to obtain certification for their relevant data processing activities and EU-based entities would then be able to rely on that certification as a 'tool to frame its transfers'.[444] With EEA-wide certification, a Northern Irish entity would be able to import data from many EEA-based entities without additional legal complication.

However, the resources required to both establish certification schemes and achieve certification are significant and obtaining certification only became a practical option

---

[439] European Commission. Directorate General for Justice and Consumers. and others, Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : Final Report. (Publications Office 2019) 176, 182 <https://data.europa.eu/doi/10.2838/115106>.

[440] EDPB, 'Guidelines 07/2022 on Certification as a Tool for Transfers' v.2.0, adopted on 14 February 2023.

[441] ibid.

[442] ibid 14.

[443] Eric Lachaud, 'Third-Party Certification and Cross-Border Flows in the GDPR: Which Workable Option?' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3686132> accessed 19 August 2023.

[444] EDPB, 'Guidelines 07/2022' (n 440) 3.

relatively recently. In October 2022, the Europrivacy certification scheme became the first certification scheme approved by the EDPB, having been submitted by the Luxembourg supervisory authority.[445] The Europrivacy certification scheme is managed by the European Centre for Certification and Privacy and is supervised by the Europrivacy International Board of Experts. The scheme was developed through the Horizon 2020 programme and is designed to apply to a 'large variety of data processing activities'.[446]

As a tool for both achieving and demonstrating compliance with the GDPR, certification offers a ‘stricter and more formalized’ approach than that offered by CoC. Accordingly, certification is likely to be an ‘expensive’ and ‘time consuming’ tool.[447] While the approval of the Europrivacy scheme by the EDPB is a significant milestone and indicates increased interest in certification as a compliance tool, it was noted by the EDPB that

> The Europrivacy certification mechanism is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.[448]

For entities in NI wishing to receive data from EEA entities, this would therefore also require effort on the EEA entities part to ensure that, in addition to the certification, any supplementary measures required to ensure adequate protection are also in place.

---

[445] EDPB, ‘Opinion 28/2022’ (n 440).
[446] Sébastien Ziegler and others, ‘Europrivacy Paradigm Shift in Certification Models for Privacy and Data Protection Compliance’ in Stefan Schiffner, Sebastien Ziegler and Adrian Quesada Rodriguez (eds), Privacy Symposium 2022 (Springer International Publishing 2022) 74.
[447] Steindl, 'Safeguarding Privacy and Efficacy' (n 430) 12.
[448] EDPB, ‘Opinion 28/2022’ (n 440).

(iv) Challenge on the Grounds of International Trade Law

Finally, for the sake of completeness, it is worth mentioning a more speculative mitigation measure: the possibility of challenging a finding of inadequacy, whether from the Commission or the CJEU, in another forum. Both the EU and the UK are members of the World Trade Organisation and signatories of relevant associated free-trade treaties. The EU's data transfer rules are frequently referred to as protectionist by their critics[449] , leading some scholars to investigate whether the application of these rules might succesfully be challenged under international trade law.

Article XIV of the General Agreement on Trade and Services (GATS) contains a 'general exception', which has been replicated in other international trade agreements. Article XIV gives signatory states the regulatory autonomy to adopt necessary measures to achieve a number of public policy objectives provided that such measures are not applied in a way that is arbitrary, unjustifiably discriminates between States or constitutes a disguised trade restriction. Amongst the public policy objectives identified are measures 'necessary to secure compliance with laws or regulations which are not inconsistent with [GATS]' including 'the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'.[450]

The EU has adopted model clauses on cross-border data flows for the digital trade chapters of its international agreements. These model clauses include a clause on privacy and data protection which is much broader than the general exception found in the GATS and explicitly refers to rules on data transfers. Such clauses must, nevertheless, themselves comply with international trade rules, in particular the GATS. There are a number of grounds on which the compatibility of the EU's transfer regime

[449] For instance, President Obama stated '..oftentimes what is portrayed as high-minded positions on issues sometimes is designed to carve out their commercial interests'. Liz Gannes, 'Obama Says Europe's Aggressiveness Toward Google Comes From Protecting Lesser Competitors', recode, 23 February 2015. Available at: https://www.vox.com/2015/2/13/11559038/obama-says-europes-aggressiveness-towards-google-comes-from.

[450] Article XIV(c)(ii).

with such rules might be challenged. For instance, it could be claimed that the adequacy process is discriminatory: the failure to review the adequacy decisions of States deemed adequate prior to the entry into force of the GDPR in light of the more stringent standards applied and assessment conducted post-GDPR might provide proof of such discrimination between States. Equally, it could be argued that the inclusion in adequacy decisions of an assessment of the national security regimes of third countries is arbitrary or reflects disguised protectionist motives as the national security regimes of EEA Member States are not taken into consideration when enabling free flows of data within the EEA. Finally, it might simply be argued that the RU regime is disproportionate and that it goes beyond what is necessary to achieve its objectives in contradiction to the necessity jurisprudence of the WTO. Trade and data protection expert Yakovleva suggests that this is the case, and that the EU finds itself in a 'compliance deadlock' torn between conflicting legal requirements: those stemming from international trade law and the EU Charter of Fundamental Rights.[451] For Yakovleva, the prospects of a successful challenge to the EU's data transfer rules on the grounds of non-compliance with international trade law are good. Nevertheless, this might provide cold comfort to data importers in NI reliant on data flows from the EU for various reasons, including the difficulty in assessing to what extent an EU trading partner might pursue legal proceedings against the EU in this way and the length of time that such proceedings would take to come to fruition. Even then, the EU's response to a negative finding is difficult to gauge.

6 Key Findings

6.1 The Significance of Data Adequacy for Northern Ireland

A loss of adequacy status would result in significant economic costs for NI and the UK. The economic evidence clearly shows that adequacy decisions have a positive economic impact. Adequacy decisions greatly simplify the free flow of data from the

[451] Svetlana Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two Necessities' [2020] Journal of World Investment and Trade 881, 886.

EEA to third countries. This facilitates greater data sharing which has positive economic effects in the form of increased of market access, trade, and investment. Furthermore, the cost burden is significantly reduced where an adequacy decision is in place. In the event of a loss of adequacy, many UK businesses and EEA partners would need to invest significantly in mitigation strategies to simply maintain existing trading relationships. This could have negative implications for the competitiveness of NI and the wider UK.

When considering the importance of adequacy for NI, it is imperative to consider its unique circumstances. A loss of adequacy would have significant and specific implications for NI due to the economic and social ties with the RoI. This report identifies three factors as particularly important when assessing the particular impact of a loss of adequacy on NI. These are:

(i) the disproportionate impact on SMEs
(ii) the consequences of a loss of adequacy for all-Island initiatives in various sectors; and
(iii) the effect a loss of adequacy may have on the ability of entities to comply with their Windsor Framework duties.

First, the report finds that a loss of adequacy would be particularly challenging for SMEs with less legal and financial resources to manage the change in circumstances. Given the NI economy's greater reliance on the success of SMEs and micro-businesses, a loss of adequacy could have disproportionate effects on the NI economy compared to other parts of the UK. Second, the impact of a loss of adequacy on all-Island initiatives, including those requiring the sharing of health and research data, is another area of specific concern to NI. Third, the Windsor Framework, a crucial instrument for the success of the NI economy, is reliant upon seamless data transfers. In the event of a loss of adequacy, meeting the traceability requirements of the Framework would be significantly more cumbersome and costly. Such a scenario has the potential to undermine the operation of the Windsor Framework.

6.2 Risks to Data Adequacy Posed by the Data Protection and Digital Information (No 2) Bill

Our analysis of the DPDI (No 2) Bill identifies four key areas of change that could potentially threaten UK data adequacy. These are changes to data protection law related to:

(i) Independence and political influence
(ii) Access to effective individual remedies
(iii) Onward transfers of personal data
(iv) Changes to the rights of individuals and other societal safeguards

(i) Independence and Political Influence

The necessity of an independent regulator is specifically provided for in the CFR and CJEU case law states that the requirement for independence is intended to 'preclude not only direct influence, in the form of instructions' but also 'any indirect influence which is liable to have an effect on the supervisory authority's decisions. The DPDI (No 2) Bill aims to reform the ICO in a number of ways that relate to the independence of the regulator. The regulator's proposed reincorporation as a body corporate – as opposed to a corporation sole – is unlikely to raise any adequacy concerns. The Bill's proposals to modify the Commissioner's statutory duties is a potential risk, however. This raises a risk that the regulator may work towards the Government priorities of innovation and competition at the expense of fundamental rights. Most significantly, the enhanced role for the Secretary of State in the setting of 'strategic priorities' and the approval of codes of practice threatens the regulator's independence as defined by the CJEU. It is difficult to reconcile the role foreseen for the Secretary of State in strategic priority setting and blocking the adoption of CoC with such freedom from influence. The Bill's provision for Government-led priorities compromises the fundamental rights orientation of the law and risks politicizing the application of data protection laws. This move, coupled with the power to obstruct regulator-proposed codes, undermines the 'complete independence' mandated by EU law.

Key finding: Changes related to independence and political influence have the potential to threaten UK adequacy status. This is likely the most significant risk to adequacy contained in the DPDI (No 2) Bill.

(ii) Access to Effective Individual Remedies

Access to individual remedies will be materially affected if the ICO's obligation to respond to complaints is modified as planned by the DPDI (No 2) Bill. Even so, it is uncertain whether this change would be deemed problematic by the Commission, particularly as there is evidence of EU supervisory authorities adopting similar strategies. Notwithstanding this, the CJEU may yet find that restricting access to complaints mechanisms in this way is incompatible with EU law. Such a finding would clarify the position and spotlight the potential issue with UK law in any review of adequacy.

Key finding: The dilution of the individual right to lodge a complaint in favour of a shift to more strategic enforcement has the potential to undermine the UK adequacy decision.

(iii) Onward Transfers of Personal Data

The provision for 'Transfers Approved by Regulations' in the DPDI (No 2) Bill acts as the UK alternative to the EU adequacy mechanism by facilitating transfers with certain third countries where they meet the standards of a 'data protection test'. Instead of adopting a standard of essential equivalence like the EU, it requires that third country protections are 'not materially lower than those offered in the UK'. The absence of a requirement to consider issues of key importance in CJEU jurisprudence – including rules on public authority access and use, independent oversight, and judicial review – before approving a third country for transfers leaves the mechanism open to challenge. Onward transfers can completely undermine an otherwise protective regime and this is reflected in the attention the Commission has given to this issue in adequacy decisions concerning other countries. Accordingly, the suggested changes will be closely scrutinised by the Commission and are likely to be found lacking. Any gap in

protection identified by the Commission would need to be addressed, but the issue could likely be remedied with additional assurances and safeguards from the UK Government.

Key finding: The DPDI (No 2) provision for onward transfers is likely to be subject to intense scrutiny by the Commission. Additional assurances and safeguards aligned with EU standards are likely to be required.

(iv) Changes to the Rights of Individuals and Other Societal Safeguards

This report identifies changes related to automated decision making, data subject rights, and mandatory DPIAs as potentially reducing the level of protection for individual and societal interests. We conclude that these changes are likely within the discretion afforded by adequacy.

Key finding: Taken individually, these changes are likely to be acceptable on the basis that the standard of adequacy is essential equivalence and not identical protection. That being said, the changes could be viewed as contributing to a general degradation in data protection rights and that could go against the UK in a holistic assessment of adequacy.

6.3 Identifying Mitigation Measures

If the UK loses its adequacy status, whether because the Commission fails to adopt a further adequacy decision at the end of the sunset period or as a result of a successful challenge to adequacy before the CJEU, data exporters to NI would need to identify potential alternative options for data transfers. This report considered these alternatives, both tested and untested, to assess their viability and made the following key findings:

(i) The Need for a Contextual Assessment

The legal analysis demonstrates that there is much uncertainty about whether the proposed DPDI (No 2) Bill changes would lead to a revocation of the UK's adequacy status. The European Commission is likely to look at these changes more favourably

while the CJEU may invalidate the adequacy decision on the grounds that the regulator lacks 'complete independence'. Any mitigation measure would need to address the particular deficiency or deficiencies identified by the Commission or CJEU: it is therefore difficult to identify appropriate mitigation measures with certainty without this contextual information. Moreover, following the CJEU's findings in *Schrems II*, it is apparent that most of the mitigation measures identified (particularly the use of contractual mechanisms, CoC or certification by data exporters and importers) will nevertheless need to be accompanied by a fact-specific assessment of the transfer. The aim of this fact-specific assessment of the transfer is to identify whether the appropriate safeguards sufficiently address the deficiencies in the third-country (here the UK) leading to inadequacy or whether 'supplementary measures' are needed. This transfer impact assessment will be highly contextual depending on factors such as the data security measures in place, the nature of the data being transferred and the scale of the data transfers. A loss of adequacy status therefore also impacts upon the application of other mitigation measures.

Key finding: A mitigation measure must be targeted to remedy the adequacy deficiency identified by the Commission or the CJEU. This contextual information is needed to identify an appropriate mitigation measure with confidence. Moreover, it follows from the CJEU's caselaw, that if alternatives to adequacy are used to facilitate data transfers to a place deemed inadequate, then the data exporter must conduct a contextual assessment to make sure these alternatives do not suffer from the same shortcomings. This means that a loss of adequacy status also impacts upon the application of other mitigation measures.

(ii) The Potential of a Bespoke Adequacy Agreement

It is possible for the European Commission to amend or tailor adequacy decisions to facilitate a finding of adequacy and there are many existing examples of such 'partial' adequacy decisions. A partial adequacy decision allows for a finding of adequacy by, for instance, limiting the scope of the adequacy decision to remove particularly problematic processing from its remit. For instance, the UK GDPR adequacy decision excludes data transferred for immigration control purposes from its scope. An analysis

of existing adequacy decisions suggests three types of bespoke adequacy agreements are possible.

First, an adequacy decision might be adopted subject to exclusions. Certain types of data might be excluded from the adequacy assessment, or the adequacy decision might specify to whom the data must be transferred (such as in Canada where only transfers to entities falling under a particular legislative framework fall within the adequacy decision). If the key issue with UK adequacy concerns the independence of the regulator, then it is difficult to envisage how data transfers might be subject to exclusions to allow for this type of partial adequacy finding.

Second, an adequacy decision might be subject to additional rules or frameworks to facilitate an adequacy finding. For instance, beneficiaries of the Japanese adequacy decision adhere to a set of Supplementary Rules that were adopted for adequacy purposes. In the UK context, such supplementary rules could address concerns about onward transfers (for instance, limiting such onward transfers completely or to specified categories of recipients) or about individual rights protection. However, supplementary measures would not easily be able to remedy more systemic deficiencies, such as concerns about the regulator's independence or complaint-handling.

Third, it is possible that an adequacy decision could be adopted on a partial geographic basis (in this instance, an adequacy decision for NI). This solution has practical, administrative and political implications that make it highly unlikely. Practically, many entities in NI will need to ensure continuing data flows with both the EU and the UK, meaning they would need to comply with dual regulatory requirements and potential additional limitations on data flows from NI to the rest of the UK. It would also likely be difficult to disentangle NI from the existing legal framework. For instance, if the issue with adequacy was regulator independence, this would require the creation of an independent regulator for NI, which would require significant financial and political support.

Key finding: It is possible for the EU Commission to adopt tailored or partial adequacy decisions. These partial decisions allow the Commission to overcome impediments to an adequacy finding by introducing exceptions to the scope of the adequacy decision, adding supplementary conditions to the adequacy decision or by recognising adequacy on a partial geographic basis. This type of bespoke arrangement might be used to address some of the concerns with the DPDI (No 2) Bill, such as the risks from onward transfers or the changes to the rights of individuals. However, a partial adequacy decision is unlikely to address more systemic issues, such as concerns about the independence of the regulator.

(iii) The Use of Contractual Mechanisms as Appropriate Safeguards

In the absence of adequacy a data transfer can take place from an EU data exporter to a non-EU data importer if 'appropriate safeguards' are put in place. Two types of contractual mechanisms are treated as 'appropriate safeguards' under the GDPR: SCCs and BCRs.

SCCs are a type of model contract adopted by the European Commission, with the most recent iteration adopted following the CJEU's decision in *Schrems II* while BCRs are a set of legal binding rules that members of a corporate group adhere to in order to ensure that appropriate protective standards are met whenever data is transferred and processed within that corporate group. The logic behind both mechanisms is that a continuity of data protection standards is guaranteed through a contractual agreement when data is transferred outside of the EU.

Both offer a good solution for data transfers where the data exporters and importers have sufficient resources and are already widely used. SCCs are the most commonly used mechanism to facilitate data transfers and may be particularly helpful when there are existing relationships between data exporters and importers (for instance, for data transfers between a government department in the RoI to a counterpart in NI). BCRs are obviously of narrower application and are therefore most likely to be used by multi-national entities.

A disadvantage of both options is their cost of implementation. BCRs have a complex approval process and require the corporate group to put in place a costly organisational compliance programme. SCCs are modular model contracts which must nevertheless be tailored to the particular transfer context and so entail costs to put them in place and monitor their application on an ongoing basis. Most of these costs fall on the data exporter, which may affect the willingness of data exporters to adopt them. However, the input of the data importer is also required in the process requiring the data importer to also have sufficient institutional capacity to rely on SCCs.

A further potential disadvantage of these options is that data exporters must still take into account the wider legal regime of the non-EU state when adopting them. The SCCs contain a clause stating that the data exporter has used reasonable efforts to determine the importer is able to implement the clauses and suggesting that there is no reason to believe that local laws or practices will affect compliance. The data export must therefore be accompanied by a type of impact assessment where the data exporter, working in conjunction with the data importer, makes an independent assessment of the adequacy of protection of the transferred data. Where deficiencies are identified, the contractual mechanism needs to introduce supplementary measures to remedy them where possible.

Key finding: The EU data protection framework allows for transfers of data to non-EU states lacking adequacy where the data exporter puts in place 'appropriate safeguards', including contractual mechanisms. The two main contractual mechanisms are SCCs and BCR. SCCs are model clauses that can be adhered to by data exporters and importers to ensure an appropriate level of data protection while BCRs are contractual provisions entered into by members of the same corporate group that serve the same purpose. These mechanisms are well-established and tested and offer a viable option for data transfers, particularly for entities with sufficient resources and data protection experience. The resources required to implement these contractual mechanisms is however a key disadvantage. A further disadvantage is that these mechanisms do not apply in a legal vacuum: the data exporter cannot ignore the wider legal context in which they apply and, following CJEU caselaw, must undertake

an assessment of whether the level of protection offered in NI is appropriate. This contributes to the cost and uncertainty of using these contractual mechanisms.

(iv) International Agreements between Public Bodies or Authorities

While contractual mechanisms such as SCCs can be entered into by public authorities and bodies, the GDPR also specifically foresees that an EEA public authority or body can transfer personal data to a third country public authority or body where a 'legally binding and enforceable instrument' is put in place. This instrument would constitute the 'appropriate safeguard' for transfer purposes. The EDPB specifies that 'international treaties, public-law treaties or self-executing administrative agreements' may be used for this purpose and that these may be entered into on a bilateral or multilateral basis. If the agreement entered into is non-binding, such as a memorandum of understanding, then the authorisation of a competent supervisory authority must be obtained.

As with SCCs and BCRs, EU law places onerous requirements on the transferring public body to assess whether the level of protection required by EU law is respected in the third country, in order to determine whether the list of safeguards included in the international agreement can be complied with in practice, taking into account the possible interference created by the third country legislation with compliance with these safeguards.

As cross-border administrative collaboration is particularly important between NI and the ROI, this may have some useful application for NI public authorities. However, the use of such arrangements raises broader legal issues around the competence to enter into binding international agreements that can be avoided by relying on SCCs. As with the other appropriate safeguards, if the issue with adequacy is the independence of the regulator then this cannot be overcome through a binding or non-binding agreement between public authorities.

Key finding: A further 'appropriate safeguard' that might apply in the absence of adequacy is an agreement between public authorities or bodies in the EEA and those in NI. This agreement should ordinarily be binding but non-binding agreements, such

as memoranda of understanding, can be used if they have obtained the approval of the relevant supervisory authority (for instance, the Irish Data Protection Commissioner if the transfer is between a public authority in the RoI to a public authority in NI). The use of such agreements may be complicated by the question of whether NI public authorities and bodies have the legal capacity to enter into binding international agreements. Moreover, like other appropriate safeguards, the use of these agreements must take into consideration whether compliance with them can ensure essentially equivalent data protection in practice due to the laws in place in NI.

(v) Reliance on the Derogations to the Adequacy Requirement Specified in the GDPR

EU data protection law does foresee circumstances where data transfers from the EU to third countries can occur even in the absence of adequacy or, as the CJEU has suggested, where there is a positive finding of inadequacy. These situations are presented as 'derogations' to the general adequacy rule. They include situations, amongst others, where the data subject gives their explicit consent having been advised of the risks of such transfer resulting from the lack of adequacy or alternative; where the transfer is necessary for the conclusion or performance of a contract; or where the transfer is necessary for important reasons of public interest.

There is some contentiousness about whether these derogations can apply to regular data transfers. A non-binding recital of the GDPR provides that some derogations (those relating to contract and legal claims) are limited to 'occasional transfers'. The EDPB recommends that other derogations be interpreted in a restrictive way in keeping with their nature as derogations. However, the CJEU has suggested that these derogations can be used as a substitute for adequacy or SCCs even when frequent large scale data transfers were at stake. The situation is complicated further by the fact that the GDPR explicitly states that all the data transfer provisions (including the provision on derogations) shall be applied in order to ensure that the level of protection it guarantees individuals is not undermined.

These derogations might be particularly useful for smaller data exporters wishing to engage in less systematic transfers from the EU to NI (such as transfers for payroll and pensions purposes for border workers). However, some legal uncertainty remains about when the derogations can be relied upon and their use entails an administrative costs (for instance, that of ensuring valid consent) for data exporters.

Key finding: EU data protection law does foresee derogations to the general rule that data can only be transferred to a non-EU entity offering an adequate level of protection. These include situations where the data subject is cognisant of the risks of the transfer but provides explicit consent; where data transfers are required for contractual purposes or for important reasons of public interest, amongst others. There remains some ambiguity about whether these derogations can be relied upon to facilitate frequent or larger scale data transfers and there are compliance costs associated with reliance on them. Nevertheless, for data importers to NI they may offer a viable and attractive option for data transfers in the absence of adequacy.

(vi) Narrowing the Definition of a 'Data Transfer' to Avoid the Need for Adequacy

The GDPR's Chapter V adequacy requirements apply in situations where there is a transfer of personal data to a third country or international organisation. The GDPR does not define 'data transfer' and so one way of potentially avoiding adequacy requirements entirely is to argue that a particular export of data does not constitute a 'data transfer'. There are two potential arguments here.

The GDPR has an expansive territorial scope: it applies not just to entities established in the EU but also those whose processing of personal data occurs in the context of the activities of an EU established controller or processor. The presence of a subsidiary selling advertising in Spain to cross-subsidise Google's search engine activities was sufficient to bring Google within the scope of the law on this basis. It also applies where a non-EU controller or processor offers goods or services to individuals within the EU or monitors their behaviour. The first argument is that there is no data transfer where data is transferred from an EU exporter to a non-EU importer to whom the GDPR already applies. The logic behind this claim is that if the GDPR already applies to this

data importer, then there is no need to apply the supplementary rules on data transfers to it. The Commission appears to support this position. However, the EDPB considers that the importer's location in a third country is determinative, rather than whether it is already subject to the GDPR via the GDPR's extra-territorial rules.

A second argument is that the data transfer rules do not apply to 'internal processing' of data, as suggested by the EDPB. It defines internal data processing as situations where the data is not made available to another controller or processor, including where such processing takes place outside the EU. The logic behind this is that the EU data controller or processor remains responsible for the data processing even once it is transferred internally within an organisation. This could potentially be relied upon by integrated entities in NI and the RoI as a ground for data sharing. However, it also remains untested and open to legal challenge on numerous fronts.

Key finding: It is possible to argue that no data transfer occurs where the data recipient in NI is already subject to the EU's GDPR because of its expansive territorial scope or because the transfer takes place internally within an organisation and does not involve any additional data controllers or processors. In both situations the logic would be that as the GDPR applies anyway, there is no need to provide an additional layer of protection by invoking the data transfer rules. The positions of relevant actors, such as the EDPB and the EU Commission, on these arguments are ambiguous and sometimes contradictory. This is therefore a higher risk option to facilitate data flows between the EU and NI than some of the others available.

(vii) The Role of Certification Mechanisms and Codes of Conduct

The GDPR foresees new forms of 'appropriate safeguards' that did not exist under earlier data protection regimes: these are CoC and certification mechanisms. CoC can be developed by bodies representing categories of controllers or processors (such as trade representatives or academic organisations) to specify the application of the GDPR in that particular sector or industry. CoC must go through an approval process, which differs depending on whether the CoC is to apply nationally, transnationally or is to be of general application throughout the EU.

This raises the question of whether entities in NI could adhere to a CoC. Where the GDPR already applies by virtue of its broad territorial reach (for instance, where a NI service provider offers goods or services to individuals in the RoI) then the NI provider should be able to sign up to relevant CoC. Where the NI data importer is not already subject to the GDPR, then it can nonetheless adhere to CoC of 'general validity' which have gone through a more rigorous approval process. In these situations the adherence of the data importer in NI would be sufficient to validate the data transfer; the data exporter would not need to sign up to the CoC.

CoC, once established, might therefore offer an attractive solution for data importers in NI keen to take control over their ability to secure data transfers from data exporters in the EU. The use of CoC does however also present challenges. There is a long and complex administrative process to be completed by the 'code owner' before the code is approved. Private sector codes also necessitate the delegation of some supervisory functions to an accredited monitoring body with appropriate expertise. The limited number of codes adopted to date suggests these are significant hurdles and confirms that this option would only be available to data importers in NI where there is a relevant code to which they could adhere.

Certification schemes are another co-regulation tool that allow data controllers to sign up to them to demonstrate their compliance with the GDPR. They can be used by data importers in NI provided that they make binding and enforceable commitments to apply appropriate safeguards and so the offer the opportunity for entities that are not subject to the GDPR to adhere to its principles when importing data. Data exporters nevertheless must confirm that the relevant certification is effective, in particular where it covers the specific transfer carried out and whether it covers data in transit. In keeping with the CJEU's Schrems II decision, the data exporter must also consider whether the certification is capable of being effective in light of the legal framework in the importer's country. As with other 'appropriate safeguards' the data exporter would need to adopt supplementary measures to tackle any shortcomings and where this is not possible certification alone cannot facilitate the transfer.

Certification is a more widely applicable option for data importers in NI who wish to show their readiness to receive data from the EU. To date, only one certification scheme has been approved by the EDPB (the Europrivacy certification scheme) however, unlike CoC, it is open to a wide variety of controllers and processors across sectors. The certification process is however said to be expensive and time-consuming which may be a deterrent for some data importers.

Key finding: CoC and certification mechanisms offer data importers the opportunity to prove their own compliance with EU data protection standards and to show they are trusted data importers. Where an entity in NI is not already subject to the GDPR, they can only adhere to CoC with general validity. There must also be a CoC appropriate to the sector concerned available to the data importer. Certification schemes are more widely applicable but only one certification scheme has been recognised so far. Both require significant resources and capacity of the data importer. Moreover, like other appropriate safeguards, the data exporter will still need to assess whether compliance with the CoC or certification mechanism is itself sufficient for adequacy or whether supplementary measures are required.

(viii) Challenging the Adequacy Assessment Under International Trade law

Finally, while not a mitigation measure as such, it is possible that the failure to recognise the UK as adequate could be challenged by the UK on the grounds that it breaches international trade law. International trade agreements provide for trade liberalisation, including data liberalisation, unless exceptions apply. One such exception, mirrored in other bilateral and multilateral agreements is the 'general exception' found in the General Agreement on Trade and Services (GATS). This exception allows signatory states the regulatory autonomy to adopt necessary measures to achieve public policy objectives, including compliance with legal frameworks to protect privacy and data protection. However, this is subject to the caveat that the measures are not arbitrary, discriminatory or disguised trade restrictions.

The EU framework for data transfers is open to challenge on several grounds. Its operation could be argued to be discriminatory (for instance, some of the States deemed adequate pre-GDPR would be unlikely to meet the more stringent criteria applied to adequacy post-GDPR but remain recognised as adequate). It could equally be argued that the inclusion of national security frameworks within the assessment of adequacy decisions is arbitrary as national security falls outside the scope of EU law. Finally, the very necessity and proportionality of the EU regime might be questioned when other lighter-touch options might achieve the same ends.

Trade experts consider that there is a good chance that the EU regime might fail to comply with the WTO's necessity requirements and that a successful challenge before the WTO is feasible. However, this offers only a medium-term solution to any loss of data adequacy as until such a legal challenge is taken and upheld the EU adequacy rules will continue to apply. Moreover, the EU would find itself caught between compliance with two legal regimes – a compliance deadlock – and it is unclear how this deadlock would ultimately be resolved.

Key finding: It is possible that the EU's data transfer regime constitutes an unnecessary interference with free trade and violates existing international trade agreements. However, this is at best a medium-term solution as until such a claim is taken and upheld the EU adequacy rules will continue to apply. Moreover, the EU would find itself caught between compliance with two legal regimes – a compliance deadlock – and it is unclear how this deadlock would ultimately be resolved.