European Parliament

EU-UK private-sector data flows after Brexit

Settling on adequacy

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Author: Hendrik Mildebrath
Members' Research Service
PE 690.536 – April 2021

EN

European Union-United Kingdom (EU-UK) data flows – the lifelines of our shared digital trade – have come under pressure following the UK's withdrawal from the EU. To take regulatory and business decisions, a clear understanding of the state of play and future prospects of EU-UK transfers of personal data is indispensable. This in-depth analysis reviews and assesses trade dealings, adequacy challenges and transfer instruments under the General Data Protection Regulation (GDPR).

AUTHOR

Hendrik Mildebrath, Members' Research Service

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please email: eprs@ep.europa.eu

The author would like to thank Norbert Lorenz, Director of the European Parliament's Legal Service, for reading and commenting on the final draft of this paper.

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Manuscript completed in April 2021.

PE 690.536
ISBN: 978-92-846-7982-9
DOI:10.2861/595569
CAT: QA-02-21-488-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Data transfers are essential for digitally enabled and digitally delivered trade in goods and services, such as cross-border financial services and e-commerce.

Upon its withdrawal from the EU on 31 January 2020, the United Kingdom (UK) became free to determine its own international trade policy, but simultaneously forfeited rights stemming from EU membership. Without a robust follow-up arrangement to the Withdrawal Agreement, the parties would have risked disruption in cross-border transfers of personal data as well as high compliance costs. However, due to lack of agreement on data transfer conditions and possible divergence in data standards, the parties were unable to implement sustainable solutions, such as long-term trade rules or an adequacy decision under the General Data Protection Regulation (GDPR). A recent study estimated the costs of 'inadequacy' at around GB£1-1.6 billion (€1.116-1.7856 billion) for UK firms, stemming largely from companies reverting to alternative transfer mechanisms under the GDPR. At the time of writing, the remaining mechanisms hardly present a reliable alternative, since they are encumbered by similar concerns to a UK adequacy decision and are partially immature, as well as narrow in scope. After lengthy negotiations, the UK and the EU agreed on a Trade and Cooperation Agreement (TCA), including an interim solution ('bridging mechanism') ensuring the provisional continuation of personal data flows. Although the interim solution is already subject to criticism from the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), it seems that supervisory authorities are willing to accept the bridging mechanism – as long as this approach is not repeated, much less becomes the norm. With the interim solution expiring on 30 June 2021, the risk of disruption and high costs has only been deferred.

Consequently, the European Commission launched the procedure for the adoption of two adequacy decisions for transfers of personal data to the UK, under the GDPR and the Law Enforcement Directive (LED) respectively, on 19 February 2021. With the publication of its draft decisions, the Commission initiated the process of adopting an adequacy decision that enables the commercial transfer of personal data without the need to obtain further authorisation. While privacy professionals, academics, supervisory authorities and civil society organisations have raised concerns that the UK's legislative framework and data-related practices may preclude an adequacy decision, the Commission considers that the UK's level of data protection is essentially equivalent to that of the EU and intends to grant the UK an adequacy decision. Specifically, the Commission attempts to dispel criticism as regards, for instance: (i) UK surveillance laws and practices; (ii) shortcomings in the implementation of EU data protection standards linked to the immigration exemption and the Digital Economy Act 2017; (iii) weak enforcement of data protection rules by the UK Information Commissioner's Office (ICO); (iv) potential liberal onward transfer of data; and (v) the UK's wavering commitment to EU data protection standards. Against this backdrop, the Commission emphasises its suspension and termination rights in case inadequacy is revealed and includes an unprecedented expiry date in the draft decision. Critics argue that the UK must first implement reforms and provide assurances before the Commission may grant an adequacy decision. One way forward may be a thorough assessment of the UK legal framework against EU standards, including CJEU case law. Where risk of non-compliance is low and legal remedies are likely effective, commitments to a specific interpretation of the law as well as assurances of compliance might suffice as a mitigation strategy. Where serious doubts regarding UK data adequacy persist, supplementary rules, including additional safeguards, could be agreed and included in the adequacy decision, to bridge the differences between the two data protection systems. In its highly anticipated (forthcoming) opinion on the draft decision, the European Data Protection Board (EDPB) will likely scrutinise the Commission's approach and provide recommendations on next steps.

Table of contents

Table of tables

1. Introduction

The importance of data transfers for digital trade cannot be overstated – both in relation to digitally enabled and digitally delivered trade in goods and services. Data transfers are essential for a wide range of activities, such as cross-border financial services, e-commerce and the consulting business. According to UK estimates,[1] exports of 'potentially information and communications technology-enabled services' in 2018 totalled approximately GB£221 billion (€249.73 billion),[2] of which EU-bound exports accounted for about 38 %. At the same time, imports of digital services stood at around GB£107 billion (€120.91 billion), with the European Union (EU) as the main origin of services (39 %). According to one trade association,[3] the UK 'facilitates 11.5 per cent of global cross-border data flows, with 75 per cent of this traffic going to the EU'. Upon its withdrawal from the EU on 31 December 2020, the UK became free to determine its own international trade policy but also forfeited rights stemming from EU membership. Without a robust follow-up arrangement to the Withdrawal Agreement, the parties would have risked disruptions in cross-border transfers of personal data and high compliance costs for businesses. After lengthy negotiations, the UK and the EU agreed on a Trade and Cooperation Agreement (TCA),[4] containing an interim solution on the continuation of personal data flows under the GDPR. This transitional data arrangement has already been criticised[5] by the LIBE committee and will need to withstand thorough[6] scrutiny by the European Parliament. In addition, objections[7] are being raised against the mutually desired long-term solution for enabling EU-UK data flows ('UK adequacy decision'),[8] whilst the expiration date of the transitional mechanism on 30 June 2021 draws ever closer. Meanwhile, companies are faced with legal uncertainty and complexity, in times marked by greater privacy awareness[9] and little to no tolerance for non-compliance, as recently demonstrated by the Court of Justice of the European Union (CJEU) *Schrems II*[10] ruling, the EDPB's rejection[11] of a grace period and the strategic complaints[12] from an advocacy group. To take regulatory and business decisions, a clear understanding of the state of play and future prospects is indispensable.

Since the current state of play is the result of time-sensitive compromises, this analysis follows a chronological approach. While the two track negotiations (trade versus adequacy talks) had very

---

1 Understanding and measuring cross-border digital trade, UK Department for International Trade and UK Department for Digital, Culture Media & Sport, 14 Mai 2020, p. 45 and pp. 48-49.

2 Based on ECB reference rate on the date of the report's publication (14 May 2020).

3 techUK, Written evidence (PBS0050), UK Parliament, July 2020, p. 6.

4 Trade and Cooperation Agreement.

5 Opinion on the Trade and Cooperation Agreement, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 5 February 2021.

6 EU-UK Trade and Cooperation Agreement: Commission proposes to extend provisional application, press release, European Commission, 10 February 2021. The Partnership Council has extended the provisional application until 30 April 2021 in Decision No 1/2021 of 23 February 2021 as regards the date on which provisional application pursuant to the Trade and Cooperation Agreement is to cease (2021/356).

7 D. Korff D. and I. Brown, The inadequacy of UK data protection law: Executive Summary, Data protection and digital competition blog, 30 November 2020.

8 Adequacy decisions, European Commission website.

9 Cf. FRA surveys on the topic 'Data protection and privacy'.

10 Judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020; H. Mildebrath, The CJEU judgment in the *Schrems II* case, At a glance, EPRS, European Parliament, September 2020.

11 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020, p. 2.

12 101 Complaints on EU-US transfers filed, NOYB website, 17 August 2020.

significant spillover effects, the rationales and underlying interests are discussed only once, where they most closely relate to the respective procedure. In a first step, the significance of trade arrangements and a potential adequacy decision are highlighted by illustrating the drawbacks and impracticalities of alternative transfer mechanisms under the GDPR. This is followed by dedicated sections on the resulting interim solution and an outlook on the desired long-term solution – a UK adequacy decision.

2. No deal, no adequacy, no transfers?

At the outset, the UK was still treated as a member of the European Union[13] for the duration of the withdrawal transition period (1 February-31 December 2020). As the deal on the EU–UK Trade and Cooperation Agreement was under discussion until the last moment and trade talks were held behind closed doors, the shape of the compromise was uncertain and even a 'no-deal' scenario was plausible. With the UK's impending departure from the EU with no agreement, the parties also risked disruptions in data flows and high compliance costs. While it was likely that the GDPR would **remain** applicable to data flows from the EU/European Economic Area (EEA) to the UK in any event,[14] without an EU-UK compromise on data flows, businesses would have had to comply with additional GDPR requirements for third-country[15] data transfers. However, the most convenient and cost-effective data transfer mechanism under the GDPR – an adequacy decision[16] – was and remains unavailable to businesses. Essentially, the parties were steering towards a scenario without trade provisions or an adequacy decision in place, to limit economic fall-out. Law-abiding[17] companies relying on data exports to the UK would have had to reconfigure operations or leverage costly and burdensome transfer mechanisms. A recent study[18] estimated the costs of inadequacy at around GB£1-1.6 billion (€1.116-1.7856 billion)[19] for UK firms, stemming largely from reverting to mitigating strategies – that is, setting up standard contractual clauses (SCCs). According to the authors, these figures are conservative estimates and do not yet include the wider economic impacts,[20] such as reduced EU-UK trade, reduced UK investments and relocation of business functions outside the UK.

2.1. Popular but elusive catch-all solutions

At the beginning of the trade negotiations, the parties were committed to reaching a long-term and cost-effective arrangement on data flows before the withdrawal transition period ended on 31 December 2020. In the course of trade negotiations, the UK proposed that the parties should fully commit to the free flow of (personal) data, whereas the EU insisted on the primacy of data protection

[13] The EU-UK Withdrawal Agreement, European Commission website.

[14] It was unlikely that the EU would concede on its high level of data protection (cf. next section) and in case of a no-deal, the GDPR would have continued to apply.

[15] Withdrawal of the United Kingdom and the EU rules in the field of data protection, Notice to stakeholders, European Commission, 6 July 2020.

[16] Adequacy decisions, European Commission website; Whereas other transfer mechanisms are costly, bureaucratic, and time-consuming to implement, an adequacy decision allows companies to transfer personal data to designated third countries, territories or specified sectors, with little to no administrative burden.

[17] Companies disregarding the new compliance requirements, while continuing operations, would have risked GDPR fines amounting up to €20 million, or 4 % of the firm's worldwide annual revenue and could not have counted on leniency from data protection authorities, courts and advocacy groups (see introduction).

[18] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

[19] Based on the European Central Bank (ECB) average reference rate for month of publication of the report (November 2020).

[20] O. Patel, Written evidence (PBS0029), UK Parliament, June 2020.

rules, including those governing and limiting cross-border transfers. On a technical level, the UK sought to prescribe very strict thresholds[21] on attempts to restrict data transfers, while the EU narrowed its commitment to a ban on data localisation requirements,[22] without prejudice to data protection and privacy measures. These distinct approaches reflected the underlying positions: arguably, the UK wanted to unleash the potential of unrestricted personal data processing and escape the disciplinary effect of the GDPR and the CJEU, while the EU aimed to uphold a high level of data protection and minimise the risk that its privacy framework might be challenged as trade protectionism on the grounds of the trade agreement (trade discipline).

Prior trade negotiations with Japan[23] reveal that it was improbable that the EU would agree to provisions that expose its GDPR data transfer mechanisms to trade discipline. In line with this, the parties began discussing a UK adequacy decision on 11 March 2020. Adequacy decisions enable companies to conveniently and cost-effectively transfer personal data to designated third countries, territories or specified sectors. Typically, these decisions impose little to no additional administrative burdens on businesses. Ultimately, 'Once the EU Commission considers a country to have an adequate level of protection, processing of data may take place just as if the processing would take place within the EU' with only a few additional steps.[24] In comparison to other transfer mechanisms available[25] under the GDPR, it is the commercially least costly[26] – although potentially equally uncertain[27] – mechanism. Pursuant to Article 45(1) GDPR, the Commission issues an adequacy decision where the respective third country, here the UK, ensures an adequate level of data protection. The level of data protection is adequate, where the standard of protection is 'essentially equivalent'[28] (not necessarily identical) to that of the EU (including the EU Charter of Fundamental Rights).[29] The European Commission must take into account such elements as respect for fundamental rights and freedoms and relevant legislation and its implementation, including concerning national security (Article 45(2) GDPR). The assessment of this condition is ongoing and the UK is currently attempting to demonstrate its adequacy with an explanatory framework.[30] At least every four years, the Commission reviews developments in third countries and may repeal, amend or suspend the adequacy decision where the third country no longer ensures an adequate

[21] According to J. Ruiz, What the UK-Japan trade deal means for digital rights, Briefing, Open Rights Group, 5 November 2020, and S. Yakovleva and K. Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade', *International Data Privacy Law*, Vol. 10(3), August 2020, the requirements 'legitimacy, trade discipline, proportionality' are much stricter than they appear and therefore present very high thresholds for any measures restricting data flows.

[22] Data localisation rules require that data shall be stored and processed within the territory of its state of origin. As regards underlying motives and effects, see J. Selby, 'Data localisation laws: trade barriers or legitimate responses to cybersecurity risks, or both?', *International Journal of Law and Information Technology*, Vol. 25(3), 13 July 2017 and R. Taylor, '"Data localization": The internet in the balance', *Telecommunications Policy*, Vol. 44(8), September 2020.

[23] The EU-Japan Economic Partnership Agreement contains a placeholder in the section 'free flow of data' (Article 8.81), requiring the parties to 'reassess within three years of the date of entry into force [...] the need for inclusion of provisions on the free flow of data' into the trade agreement. Japan, however, did receive an adequacy decision enabling data transfers from the EU/EEA to Japan and including onward data transfers.

[24] M. Lachenmann, Data transfers between the EU and Japan: an introduction to the EU's adequacy decision on Japan, LinkedIn, 2 July 2019.

[25] Standard contractual clauses, binding corporate rules, derogations for specific situations, approved codes of conduct, an approved certification mechanism.

[26] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

[27] O. Patel and N. Lea, EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, UCL European Institute, May 2020, p. 29.

[28] Judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020, para. 94.

[29] Charter of Fundamental Rights of the European Union.

[30] Explanatory framework for adequacy discussions, Policy papers, UK Government, 13 March 2020.

level of protection. However, due to concerns regarding the UK's level of data protection (see section on 'The adequacy decision – a viable long-term solution?' below), the EU has only recently, on 19 February 2021, launched[31] the procedure for the adoption of an adequacy decision (see Box 1). Consequently, the decision is not yet in effect and companies cannot rely on this mechanism for EU-UK data transfers today.

Box 1 – Procedure for adopting adequacy decisions

Pursuant to Article 45(1) GDPR, the Commission issues an adequacy decision where the respective third country, here the UK, ensures an adequate level of data protection. According to Article 45(3) in conjunction with Article 93(2) GDPR, the assessment is taken unilaterally by the European Commission's Directorate-General for Justice and Consumers (DG JUST), following a non-binding opinion from the European Data Protection Board (EDPB) according to Article 70(1)(s) GDPR. After obtaining approval for its draft decision from the 'Article 93 Committee', consisting of Member States' representatives, the Commission must adopt the act (Article 93(2) GDPR in conjunction with Article 5(2) Regulation (EU) No 182/2011, which establishes the 'examination procedure'). If the committee delivers a negative opinion with a qualified majority (55 % of EU countries representing at least 65 % of the total EU population), the Commission shall not adopt the draft implementing act (Article 5(3) Regulation (EU) No 182/2011). Where an implementing act is deemed to be necessary, the chair (representative of the Commission) may either submit an amended version of the draft implementing act to the same committee within two months of delivery of the negative opinion, or submit the draft implementing act within one month of such delivery to the appeal committee for further deliberation. The European Parliament and the Council should simultaneously receive information regarding actions taken in committee (right of information, Article 10(3) and Recital 17 Regulation (EU) No 182/2011), and can request that the Commission maintain, amend or withdraw an adequacy decision at any time if they perceive the Commission is exceeding its implementing powers under Article 45 GDPR (right of scrutiny, Article 11 Regulation (EU) No 182/2011). Currently, 12 countries benefit from an adequacy decision. Recently, the CJEU invalidated the United States adequacy decisions in its 2020 *Schrems II* judgments.

In the course of adopting a domestic replication of the GDPR ('UK GDPR'), the UK also introduced a national adequacy mechanism. The UK has transitionally issued the EU data adequacy, to enable the convenient **export** of personal data **to** the EU (this does not cover the **import** of data **from** the EU).

2.2. Sub-optimal mitigation strategies

Other transfer mechanisms provided for in the GDPR are considered to be impractical, immature, uncertain, risky or costly.[32] Depending on businesses' awareness, compliance resources and cost-benefit analysis, they might instead resort to non-compliance, data (re-)localisation,[33] limiting transfers to anonymised data, or halting transfers altogether.

2.2.1. Standard contractual clauses (SCCs)

Currently, by far the most popular among the remaining GDPR transfer mechanisms are the **standard contractual clauses (SCCs)**. Companies may transfer data to third countries on the basis of template contract terms adopted by the Commission in accordance with Article 46(2)(c) in

[31] International dimension of data protection > Brexit, European Commission website.

[32] For instance T. Christakis, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers Part 1 / Part 2 / Part 3, European Law Blog, 13-17 November 2020; D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

[33] A. Chander, 'Is Data Localization a Solution for Schrems II?', *Journal of International Economic Law*, Vol. 23(3), 5 September 2020.

conjunction with Article 93(2) GDPR.[34] A privacy professional association found[35] that 88 % of survey respondents whose organisations move personal data outside of the EU rely on standard contractual clauses (SCCs). Ultimately, the UK Government[36] and the majority of commentators[37] also expect that standard contractual clauses would be leveraged in the event that adequacy is not issued. In practice, they are often already in place as a precautionary measure, even where business could rely on an adequacy decision, since the Commission may amend or suspend these adequacy decisions (Article 45(5) GDPR). Nevertheless, deploying or updating these contracts is currently a delicate matter, since (i) it is **uncertain** which type of safeguards suffice to salvage **potential** UK privacy lacunae, resulting in a two-fold uncertainty, and (ii) the Commission is currently revising the SCCs. Not to mention that large companies will likely need to update hundreds or even thousands[38] of contracts, meaning updates should be done correctly the first time to avoid costs, making certainty and a structured approach essential.

(i) According to the recent *Schrems II*[39] ruling, data transfers based on SCCs do not per se present lawful transfers. Controllers and processors must ensure that data subjects whose personal data is transferred to a third country are afforded a level of protection **essentially equivalent** to that guaranteed within the EU. They must take into account jointly agreed contractual guarantees and safeguards, as well as the relevant aspects of the third-country legal system pertaining to, for instance, the data access rights of public authorities. Where the third country does not afford an equivalent level of data protection, the operators must provide for additional safeguards to compensate the privacy lacunae. Since contractual clauses do not bind third parties and national authorities ('privity of contracts'), the EDPB recommends,[40] inter alia, strong encryption mechanisms.[41] The Board[42] seems to have rejected[43] proposals[44] for a risk-based approach and raises concerns on the suitability of purely contractual or organisational measures as a means to impede access by public authorities, for instance, national intelligence measures. While technical safeguards

[34] Subject to authorisation from the competent authority (Articles 46(3)(a) and (4) GDPR), controllers and processors may also rely on custom contractual clauses. If standard clauses are adapted, replaced or deleted to deviate substantively from the standard contract terms, they also become subject to the approval procedure.

[35] IAPP-EY Annual Governance Report 2019, International Association of Privacy Professionals (IAPP) and Ernst and Young (EY), 2019.

[36] Department for Business, Energy and Industrial Strategy, Written evidence PBS0024, UK Parliament, June 2020.

[37] E.g. D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

[38] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020, p. 20.

[39] Judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020; H. Mildebrath, The CJEU judgment in the *Schrems II* case, At a glance, EPRS, European Parliament, September 2020.

[40] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020.

[41] See T. Christakis, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers Part 1 / Part 2 / Part 3, European Law Blog, 13-17 November 2020, for contextualisation in European Court of Human Rights (ECtHR) and CJEU case law.

[42] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020, p. 15.

[43] T. Christakis, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers Part 2, European Law Blog, 16 November 2020.

[44] See for instance A path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision, Centre for Information Policy Leadership (a think-tank that counts 81 member companies and project participants), 24 September 2020.

seem promising, this may produce additional costs or conflict[45] with business cases.[46] Failing to provide for an equivalent level of protection, operators must suspend data transfers. Supervisory authorities must check transfers and are 'required' to suspend or prohibit transfers where they find that data subjects are not afforded essentially equivalent protection, pursuant to Article 58(2)(f) and (j) GDPR. Essentially, companies and their legal counsels would need to assess the level of data protection in the recipient country ('private adequacy assessment') and discern how potential lacunae might be adequately compensated – two very challenging tasks.[47]

(ii) Currently, the Commission is seeking to replace the 2001, 2004 and 2010 SCCs[48] with a single implementing decision[49] comprising a modular approach, addressing constellations where data transmitter and data receiver qualify as either controller or processor. Together, the EDPB and European Data Protection Supervisor (EDPS) published[50] a joint opinion on the Commission's draft decision[51] on 14 January 2021.

In other words, at the time of writing, there is a high degree of uncertainty as regards data transfers based on SCCs and a reliable best practice has not yet emerged.

2.2.2. Binding corporate rules (BCRs)

While SCCs may be leveraged for most international data transfers, notably between groups and legal entities, Binding corporate rules (BCRs) are applicable to transfers of personal data outside the EEA but only within a group of undertakings or enterprises.[52] They allow companies to transfer personal data to their (intra-group) affiliates located outside the EEA. These data protection policies must be legally binding and enforced by every member of the group (including their employees), expressly confer enforceable rights on data subjects and further stipulate minimum requirements laid down in Article 47(2) GDPR, notably a data protection audit mechanism. Essentially, they place[53] 'an obligation on the entire organisation to comply with and adhere to pre-approved data protection standards'. They are usually modelled on a set of Article 29 Working Party (precursor to

---

[45] T. Christakis, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers Part 2, European Law Blog, 16 November 2020.

[46] As reported, one independent cybersecurity researcher held 'In general, encryption in and of itself may likely not be sufficient either because there always needs to be a way to decrypt data, for example, to have it usable'. He considers that a combination of technological and organisational changes may be a way forward. One company relies on a combination of measures, including a commitment to challenge every government data request in court (where there is a lawful basis for doing so), providing customers with monetary compensation in case of disclosure in violation of the GDPR, encryption measures and transparency measures.

[47] In the (translated) words of CJEU Judge Thomas von Danwitz (European Data Protection Day, 2:46:02-2:47:57): *'The adequacy decision has a big advantage for companies because this means they have no problem. As long as such a decision is valid, they can transfer without any further checks or controls, whereas with standard contractual clauses or similar guarantees you have to check in every individual case [...]. Then, in every individual case, the company has to [...] make sure that the transfer is carried out in such a way that the rights of the data subject are protected at a level that is similar to the protection level of the EU. And for many companies, in particular small and medium-sized companies that is a heavy burden, but that is what the GDPR demands.'*

[48] Standard Contractual Clauses (SCC), European Commission website.

[49] Draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, public consultation, European Commission, 12 November 2020.

[50] Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, European Data Protection Board and European Data Protection Supervisor, 14 January 2021

[51] Draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, public consultation, European Commission, 12 November 2020.

[52] For details on the meaning of 'a group of undertakings or enterprises' see N. Werry N. and S. Werry, *'Internationaler Transfer personenbezogener Daten'*, in L. Specht-Riemenschneider et al., *Datenrecht in der Digitalisierung*, Erich Schmidt Verlag, 2020, p. 115.

[53] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

the EDPB) working documents.[54] Once they have been approved by the supervisory authority in accordance with the consistency mechanism, Articles 47(1), 63 and 64(1)f) GDPR, individual data transfers do not require further approval. According to the EDPB[55] and the Conference of the German Data Protection Authorities (DSK),[56] companies will equally need to ensure a level of data protection essentially equivalent to that guaranteed by the GPDR and the EU Charter of Fundamental Rights – if necessary with additional measures to compensate for lacunae in the protection of third-country legal systems. This point has been reinforced[57] by recent post-*Schrems II*[58] EDPB opinions[59] on BCRs. Consequently, companies opting for BCRs would likely face similar challenges in assessing foreign standards of data protection and compensating privacy lacunae with uncertain additional safeguards, as companies relying on SCCs. In principle, setting up BCRs is 'more costly and burdensome for organisations than setting up SCCs' and may increase the 'risk' of revealing own-non-compliance in the course of mandatory audits.[60] Nevertheless, very large firms may prefer to set up BCRs, for instance, where a large-scale investment is more cost-effective, to demonstrate accountability or where changing corporate structures or complex webs of data processing require flexibility. Only a few large multinational corporations operating across borders use BCRs.[61]

2.2.3. Article 49 GDPR derogations

Although the EDPB recognises[62] that it is possible to transfer data on the basis of derogations envisaged under Article 49 GDPR, its guidelines[63] raise doubts as to the lawfulness and practicability of this approach as a basis for recurrent data transfers outside the EEA. The document argues that for companies it is impractical to rely on consent pursuant to Article 49(1)(a) GDPR for data transfers, since (i) the requirements of an explicit and informed consent are difficult to satisfy (Articles 6(11) and 7 GDPR), (ii) consent remains revocable (according to EDPB's interpretation of Recital 111 GDPR and Article 49(1) subpara. 2 GDPR), and (iii) Article 49(1)(a) GDPR only legitimises **occasional** and not systematic transfers. Also, other derogations that might be considered as legal bases, such as Articles 49(1)(b) and 49(1)(c) GDPR, are only applicable to occasional transfers and therefore impractical for businesses. However, certain commentators dispute that this exception is effectively

---

54 Binding Corporate Rules (BCR), European Commission website.

55 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020; Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020, p. 18.

56 Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger, press release, German Data Protection Authorities (DSK), 28 July 2020.

57 J. Tielemans, BCRs after 'Schrems II' decision: A first analysis, The Privacy Advisor, IAPP, 27 October 2020.

58 Judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020; H. Mildebrath, The CJEU judgment in the *Schrems II* case, At a glance, EPRS, European Parliament, September 2020.

59 Register of approved binding corporate rules, European Data Protection Board website.

60 D. McCann et al., *The cost of data inadequacy* (November 2020), p. 7; C. Schröder, 'Artikel 47 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG Kommentar*, C.H.Beck, 2018, para. 49.

61 On 6 October 2017, The UK Information Commissioner's Office had authorised the transfers of personal data under Binding Corporate Rules for 32 entities; A Commission document, providing an overview of companies for which the BCR cooperation procedure was closed by 24 May 2018, lists 132 companies. The EDPB register of approved binding corporate rules contains seven undertakings/enterprises.

62 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020, p. 3.

63 Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, European Data Protection Board, 25 May 2018.

limited to occasional transfers only.[64] Additionally, CJEU Judge Thomas von Danwitz, the Rapporteur for the *Schrems II* and the *La Quadrature du Net and Others*[65] rulings, suggested[66] that these derogations may apply more widely than expected, particularly as regards intra-group transfers.

2.2.4. Codes of conduct

Codes of conduct for third-country data transfers, pursuant to Articles 46(2)e and 40(2)(j) GDPR, are still at an early stage. While some commentators see great potential in these codes,[67] practical examples are still emerging.[68] These codes will likely be used to transfer data between entities that have subscribed to the same (approved)[69] code.[70] The controller or processor in the third country must have committed to the code and its enforcement in a binding manner, particularly through contractual arrangements.[71] Accredited independent bodies will monitor the compliance with such codes, Articles 40(4) and 41(1) GDPR. As the codes are not restricted to intra-group transfers, they cover more processing operations than BCRs. However, as with SCCs and BCRs, where businesses want to transfer data to third countries, they will likely[72] need to ensure a level of data protection essentially equivalent to that guaranteed by the EU data protection *acquis*. Where codes support the transfers to countries lacking an adequate level of data protection, they should ideally set out practical rules for additional safeguards and thereby support or relieve businesses from private adequacy assessments and deliberations as to how potential privacy lacunae might be compensated.[73] Notwithstanding, the reliability of these supplementary measures remains uncertain and the subscription to these codes does not reduce the responsibility of the controller or processor for compliance with the GDPR.[74] However, their deployment may relax the burden of proof for compliance (e.g. Articles 24(3), 28(5) or 32(3) GDPR) and serve as an attenuating circumstance in the face of fines (Article 83(2)(j) GDPR). Similar to BCRs, they demonstrate

[64] D. Pauly, 'Artikel 49 DS-GVO', in B. Paal and D. Pauly, *DS-GVO BDSG*, C.H.Beck, 2021, para. 2; C. Schröder, 'Artikel 49 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG Kommentar*, C.H.Beck, 2018, para. 12.

[65] Judgment in Joint-Cases C 511/18, C 512/18 and C 520/18 – *La Quadrature du Net and Others*, CJEU, 6 October 2020.

[66] CJEU Judge T. von Danwitz, European Data Protection Day 2021, 28 January 2020, 2:23:11-2:27:06; R. van Eijk and G. Zanfir-Fortuna, Schrems II: Article 49 GDPR derogations may not be so narrow and restrictive after all?, Future of Privacy Forum Blog, 4 February 2021.

[67] C. Witt et al., Could codes of conduct be the answer to 'Schrems II'?, The Privacy Advisor, IAPP, 29 September 2020.

[68] Third Country Transfer Initiative, EU Cloud CoC website; N. Werry and S. Werry, 'Internationaler Transfer personenbezogener Daten', in L. Specht-Riemenschneider et al., *Datenrecht in der Digitalisierung*, Erich Schmidt Verlag, 2020, pp. 134-135.

[69] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, European Data Protection Board, 4 June 2019; WP29, Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?, DG XV D/5057/97 final, Article 29 Data Protection Working Party, 14 January 1998.

[70] L.-M. Lange and A. Filip, 'Artikel 46 DS-GVO', in H. A. Wolff and S. Brink, *BeckOK Datenschutzrecht*, C.H.Beck, 1 November 2020, para. 49; This is arguable, since Article 46(2)(e) GDPR only requires that the controller or processor in the third country commits to apply the appropriate safeguards, including as regards data subjects' rights. Additionally, the interplay of codes of conduct and potential compatibility remains underexplored.

[71] L.-M. Lange and A. Filip, 'Artikel 46 DS-GVO', in H. A. Wolff and S. Brink, *BeckOK Datenschutzrecht*, C.H.Beck, 1 November 2020, para. 51.

[72] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020 and *Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger*, press release, Conference of the German Data Protection Authorities (DSK), 28 July 2020; Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020, p. 18.

[73] See J. Wittmann, Webinar: Implementing Codes of Conduct - Sharing Practical Experiences in Co-Regulation for Third Country Transfers post Schrems II, EU Cloud CoC, 24 February 2021,12:27-16:43.

[74] M. Bergt, 'Artikel 40 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG Kommentar*, C.H.Beck, 2018, para. 43.

compliance and accountability towards business partners and consumers, but unlike BCRs, they will also be available to companies with less means. Another advantage is that these codes are developed in a sector-specific manner and will likely be accompanied by implementation guidelines. Arguably, their introduction raises procedural questions.[75] Potentially, not all associations will have the means to develop such codes and not all actors (e.g. small and medium-sized enterprises (SMEs)) possess the negotiating power to see their interests reflected in relevant codes.[76] The EDPB has announced[77] that it will provide separate guidelines in relation to the use of codes as a mechanism to facilitate transfers. This was initially planned[78] for 2019-2020, but no guidelines have been issued to date.

2.2.5. Certification mechanism

In the future, companies may leverage the certification mechanism set out in Articles 42 GDPR for third country transfers pursuant to Article 46(2)(f) GDPR. Similar to codes of conduct, this transfer mechanism is still at an early stage and not practically available to businesses.[79] Where businesses seek to export data to third countries based on Article 46(2)(f) GDPR, they will need to successfully complete a certification procedure pursuant to Article 42 GDPR, and the controller or processor in the third country must make binding and enforceable commitments to apply the appropriate safeguards. This certification procedure requires that applicants' operations and data processing conform to GDPR requirements, notably, that appropriate safeguards are in place,[80] including[81] supplementary measures to compensate privacy lacunae of third countries where they fall short of the EU data protection standard. Upon the successful completion of the certification procedure the accredited[82] certification body would issue a statement of GDPR conformity (certification) and potentially grant the use of a logo or symbol signifying the successful complete of the certification procedure (seal or mark).[83] The former Federal Commissioner for Data Protection and Freedom of

[75] K. Schlender, 'Artikel 46 DS-GVO', in S. Gierschmann et al., *Kommentar DS-GVO*, Bundesanzeiger Verlag, 2017, para. 13-15.

[76] A. Roßnagel, 'Artikel 40 DSGVO', in S. Simitis et al., *Datenschutzrecht*, Nomos, 2019, para. 88.

[77] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, European Data Protection Board, 4 June 2019.

[78] EDPB Work Program 2019/2020, European Data Protection Board, 12 February 2019, p. 2.

[79] Cf. EDPB, *Register of certification mechanisms, seals and marks*.

[80] Bergt in Kühling and Buchner, *DS-GVO BDSG Kommentar* (2018), 'Artikel 42 DS-GVO', para. 14.

[81] According to Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020, p. 18; Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020 and Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger, press release, German Data Protection Authorities (DSK), 28 July 2020, the rationale of the Schrems II ruling is likely applicable. Certification bodies seem to be aware that the ruling will affect them.

[82] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), European Data Protection Board, 4 June 2019; A. Gühr et al., 'Der lange Weg zur Akkreditierung nach Art. 42 DSGVO', Datenschutz und Datensicherheit, Vol. 44(10), 2020, pp. 649-653; N. Maier et al., 'Die Zertifizierung nach der DS-GVO', in *Zeitschrift für Datenschutz*, Vol. 10(9), 2020, pp. 445-449.

[83] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, European Data Protection Board, 4 June 2019, p. 8; G. Hornung, 'Artikel 42 DSGVO', in M. Eßer, *Auernhammer DSGVO BDSG*, 2020, para. 2 and 36 et seq.

Information of Germany reported[84] from an event[85] that the German Accreditation Body (DAkkS)[86] has received approximately 80 accreditation[87] applications from (aspiring) certification bodies.[88] While accredited certificates do not reduce the responsibility of the controller or the processor for compliance with the GDPR (Article 42(4) GDPR), they relax the burden of proof for compliance (e.g. Articles 24(3), 25(3), 28(5) or 32(3) GDPR) and serve as an attenuating circumstance in the face of fines (Article 83(2)(j) GDPR).[89] Advocates additionally emphasise advantages,[90] such as that certification criteria and bodies provide business with support on implementing the GDPR and certificates inspire consumer trust and confidence in business-to-business (B2B) relationships. However, the certification process might be too costly for SMEs.[91] It may also require sensitive on-site inspections and code review.[92] The EDPB has announced,[93] that it will 'publish separate guidelines to address the identification of criteria to approve certification mechanisms as transfer tools to third countries or international organisations in accordance with Article 42(2)'.

Against the backdrop of the *Schrems II* ruling, concerns on the UK's level of data protection render the remaining GDPR transfer mechanisms vulnerable to challenge[94] and therefore cast serious doubt on their reliability. It remains to be seen whether the European Commission, supervisory authorities, associations and certification bodies will provide business with more extensive and practical solutions that would comprehensively address these reliability concerns, rather than high-level and generic rules or guidance.[95] The Centre for Information Policy Leadership drew up a risk-based toolkit of possible supplementary measures, including legal and organisational measures,[96] but the EDPB held that 'there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for

---

[84] 'Es liegen bisher ca. 80 Akkreditierungsanträge bei der #DAkkS vor, teilt Frau Pawlowska auf der #EAID-Veranstaltung zur #Datenschutzzertifizierung mit', Tweet on EAID event Datenschutz – Zertifizierung – Quo Vadis?, Peter Schaar.

[85] Datenschutz – Zertifizierung – Quo Vadis?, European Academy for Freedom of Information and Data Protection website, 2 March 2021.

[86] Deutsche Akkreditierungsstelle GmbH website.

[87] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), European Data Protection Board, 4 June 2019.

[88] Cf. for instance datenschutz-cert, auditor-cert and EuroPriSe.

[89] For details see B. Paal and L. Kumkar, 'Artikel 42 DS-GVO', in B. Paal and D. Pauly, *DS-GVO BDSG*, C.H.Beck, 2021, para. 9.

[90] A. Duisberg, 'Zertifizierung und der Mittelstand – Quo Vadis?', Zeitschrift für Datenschutz, Vol. 9(2), 2018, p. 53; A. Gühr et al., 'Der lange Weg zur Akkreditierung nach Art. 42 DSGVO', Datenschutz und Datensicherheit, Vol. 44(10), 2020, p. 650; L.-M. Lange and A. Filip, 'Artikel 46 DS-GVO', in H. A. Wolff and S. Brink, *BeckOK Datenschutzrecht*, C.H.Beck, 1 November 2020, para. 55-58; M. Bergt, 'Artikel 42 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG Kommentar*, C.H.Beck, 2018, para. 27-28.

[91] A. Duisberg, 'Zertifizierung und der Mittelstand – Quo Vadis?', Zeitschrift für Datenschutz, Vol. 9(2), 2018, p. 54.

[92] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, European Data Protection Board, 4 June 2019, p. 11.

[93] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, European Data Protection Board, 4 June 2019.

[94] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020, p. 12: 'SCCs and BCRs are also vulnerable to challenge since they cannot offer protection against foreign governments' surveillance and intelligence-gathering activities'; Similarly, Draft motion for a resolution on Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") - Case C-311/18, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 13 January 2021, para. 8.

[95] Draft motion for a resolution on Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") - Case C-311/18, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 13 January 2021, para. 7 suggests 'a toolbox of supplementary measures, e.g. security certification and encryption safeguards, that are accepted by regulators'.

[96] A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision, Centre for Information Policy Leadership, 24 September 2020, p. 11-15.

surveillance purposes'[97]. Beyond this, the narrow scope and immature state of certain transfer mechanisms hampers their deployment. While the selection of appropriate transfer mechanism was already a demanding task before the *Schrems II* ruling, businesses and their counsels now find themselves in a predicament.

Additionally, alternative transfer mechanisms entail non-negligible disadvantages for businesses ('costly, bureaucratic, and time-consuming to implement'[98]) and the cost of inadequacy is estimated[99] at around GB£1-1.6 billion (€1.116-1.786 billion) for UK firms, alongside wider adverse effects[100]. Moreover, the lack of an adequacy decision subjects companies to the compliance requirements of Article 71 of the Withdrawal Agreement. Accordingly, businesses must process any non-UK citizen's data, which had been transferred to the UK during its EU membership or within the transition period ('legacy data'), according to the GDPR as it stood on 31 December 2020 ('frozen GDPR').[101]

Consequently, the negotiating parties were caught in a dilemma: even if the UK conceded on the free flow of personal data and the GDPR transfer mechanism applied, an adequacy decision was out of reach (see section on 'Doubts regarding UK data adequacy'), threating to produce severe economic drawbacks.

[97] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020, p. 15-17.

[98] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020, p. 2.

[99] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020.

[100] 'Chapter 9: Digital trade and data flows', in *The future UK-EU relationship on professional and business services*, UK Parliament's European Union Committee, 13 October 2020.

[101] What is the Frozen GDPR and when does it apply?, UK Information Commissioner's Office website.

Table 1 – Benefits and drawbacks of GDPR data transfer mechanisms

Transfer mechanism	Description	Advantages	Drawbacks
Adequacy decision	Companies may transfer personal data to third countries, for which the Commission has issued an adequacy decision, reaffirming that it considers that the level of data protection in the third country is essentially equivalent to that of the EU.	- No further authorisation is required - No additional bureaucracy	- Uncertainties regarding the reliability of adequacy decisions - Only 12 countries have been granted an adequacy decision to date
Standard contractual clauses	Companies may transfer data to third countries based on template contract terms adopted by the Commission (SCCs) in accordance with Article 46(2)(c) in conjunction with Article 93(2) GDPR.	- Can be deployed off-the-shelf - May be leveraged for transfers to third countries which have not been issued with an adequacy decision or as a precautionary measures	- A private assessment of third-country data adequacy is required - Uncertainties regarding the reliability of 'additional safeguards' remain - SCCs are currently under revision - SCCs may produce substantial contract management costs - SCCs provide limited flexibility, as deviations may trigger authorisation requirements and they leave little room for generic descriptions
Binding corporate rules	Companies may transfer personal data to their (intra-group) affiliates located outside the EEA based on legally binding data protection policies approved by the competent supervisory authority.	- For multinational corporations a large-scale investment in setting up BCRs may be more cost-effective - They demonstrate compliance and accountability towards business partners - May be leveraged where changing corporate structures or complex webs of data processing require flexibility	- A private assessment of third-country data adequacy is required - Uncertainties regarding the reliability of 'additional safeguards' remain - BCRs only enable intra-group transfers - Costly to set up - Mandatory audit mechanisms act as a deterrent
Derogations	Companies may transfer data based on the statutory derogations in Article 49 GDPR.	- These derogations do not require additional guarantees - Derogations are an efficient solution at least for occasional transfers - Suitable where SCCs and BCRs cannot be introduced and an adequacy decision is absent, e.g. where an e-commerce provider is established in a third country	- The requirements are applied restrictively and are partially impractical - Arguably, they only provide grounds for occasional, not systematic, transfers

Codes of conduct	These codes will likely be used to transfer data between entities that have subscribed to the same (approved) codes of conduct. The controller or processor in the third country must have committed to the code and its enforcement in a binding manner.	- Codes of conduct cover more transfer operations than BCRs (extra-group transfers) - Codes may privilege the operator as regards GDPR requirements and fines - Codes demonstrate compliance and accountability towards business partners - Where codes address transfers to countries lacking an adequate level of data protection (e.g. universal codes), they likely set out rules for additional safeguards - Codes are developed in a sector-specific manner and are likely accompanied by implementation guidelines - Codes are available to companies that do not have the means to introduce BCRs	- These codes are still in the process of emerging. Arguably, procedural questions remain. - Likely, not all associations and other bodies will have the means to develop these codes - Uncertainties regarding the reliability of 'additional safeguards' remain
Certification mechanism	Where businesses seek to export data to third countries based on Article 46(2)(f) GDPR, they will need to successfully complete a certification procedure pursuant to Article 42 GDPR and the controller or processor in the third country must make binding and enforceable commitments to apply the appropriate safeguards.	- Certification may privilege the operator as regards GDPR requirements and fines - Certification may inspire consumer trust and confidence in B2B relationships - Certification criteria and bodies may provide business with support on the implementation of the GDPR - An ex-ante certification mechanism may mitigate future compliance risks	- Certification is not yet available to companies - Certification may be too costly for SMEs - Certification may require sensitive on-site inspection and code review - A private assessment of third-country data adequacy is required - Uncertainties regarding the reliability of 'additional safeguards' remain

The colour coding indicates a **generalised** assessment of the **current** useability of GDPR transfer mechanism for data transfers from the EEA to the UK: green = suitable; yellow = limited suitability (uncertainties); orange = very limited suitability (restricted use cases/uncertainties); red = wholly unsuitable (unavailable). This does not indicate their use case-specific or future potential.
Source: EPRS, authors' own elaboration based on sources cited in the text above.

3. The temporary bridge – A contingency measure

The parties resolved this dilemma by maintaining the applicability of their respective data protection and privacy rules, but modifying the GDPR's conventional ramifications. This interim solution is meant to pave the way to an adequacy decision.

The UK and the EU compromised on wording,[102] but essentially opted for the EU model (Chapter 2).[103] They placed a ban on data localisation requirements, but prescribed the (arguable)[104] primacy of data protection and privacy rules over all other trade provisions, provided that these rules (i) are genuinely adopted for the protection of personal data and (ii) contain data transfer mechanisms of general – not arbitrary or country-specific – application (Article DIGIT.7(2) TCA).[105] In fact, any transfer of personal data covered by the agreement will have to comply with the transferring Party's rules on international transfers of personal data, where this is not particularised in certain chapters (Article COMPROV.10(4) TCA).[106] To ensure the smooth continuation of EU-UK transfers without an adequacy decision, the parties included a 'bridging mechanism'[107] in the final provisions of the TCA, which transitionally preserves the status quo as regards transfers to the UK (Article FINPROV.10A TCA).[108] The mechanism stipulates that 'transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law'. Essentially, it delays the applicability of additional requirements intended for transfers to third countries, among which the UK now qualifies,[109] for up to six months following the entry into force of the Agreement (Article FINPROV.11 TCA),[110] or until the European Commission adopts an adequacy decision. However, this does not present a blanket authorisation for transfers since the remaining GDPR provisions continue to apply and the bridge is suspended should the UK change its data protection legislation as it stands on 31 December 2020, or exercise international transfer powers without the agreement of the EU. As part of the TCA, for which the Commission has 'chosen'[111] Article 217 TFEU as the legal basis ('association agreement'), the mechanism outranks[112] secondary law, such as the GDPR, but must be consistent with primary law, such as the EU Charter of Fundamental Rights. The LIBE committee has already expressed[113] 'strong doubts as to whether this interim regime would provide the required level of protection to the personal data transferred to the UK, as it relies on the assumption that UK data protection law currently in force has properly and correctly implemented Union data protection law [...] and that at present the UK ensures the

[102] Article DIGIT.7(2) TCA: 'Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of persona data and privacy [...], *provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the for the protection of the data transferred*' (emphasis added). In its Opinion on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, para. 16-20, the EDPS criticises this approach, since the wording in Article DIGIT. 7(2) does not fully safeguard the EU's autonomy in **how** it designs its protection of personal data and privacy, nor does it comprehensively shield all data protection provisions from challenge in trade disputes. The EDPS also suggests that uncertainties remain as regards the relations between Article DIGIT.7 TCA and Article DIGIT.4 TCA in conjunction with Article EXC.1(2)(c) TCA as well as between Article DIGIT.7 TCA and Article COMPROV.10(4) TCA.

[103] Chapter 2 TCA.

[104] The EDPS holds that it 'appears not to be excluded' that the EU's autonomy is limited [by the conditions laid down in Article EXC.1(2)(c) TCA].

[105] Article DIGIT.7(2) TCA.

[106] Article COMPROV.10(4) TCA.

[107] Using personal data in your business or other organisation, Guidance, UK Government's Department for Digital, Culture, Media & Sport, the Department for Business, Energy & Industrial Strategy, and the Information Commissioner's Office, 31 December 2020.

[108] Article FINPROV.10A TCA

[109] Withdrawal of the United Kingdom and the EU rules in the field of data protection, Notice to stakeholders, European Commission, 6 July 2020.

[110] Article FINPROV.11 TCA

[111] Questions & Answers: EU-UK Trade and Cooperation Agreement, European Commission website, 24 December 2020.

[112] European Union (EU) Hierarchy of Norms, Glossary of summaries, European Commission.

[113] Opinion on the Trade and Cooperation Agreement, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 5 February 2021, p. 5.

same level of protection set forth by the Union'. A civil society organisation cautions[114] that the legality of such an 'unprecedented workaround' is unclear. The EDPS stresses 'that such mechanism should remain exceptional and should not set a precedent for future TCAs with other third countries'.[115] The Commission will attempt to issue an adequacy decision, within the interim period, ending at the latest on 30 June 2021. In the long term, EU-UK data transfers will chiefly be determined by the unmodified third country transfer mechanisms available under the GDPR, including, if successfully adopted, an adequacy decision. With the interim solution expiring on 30 June 2021, the risk of disruption and high cost has only been deferred.

4. The adequacy decision – A viable long-term solution?

The EU and the UK began discussing an 'adequacy decision' on 11 March 2020, long before the expiration of the withdrawal period on 31 December 2020. On 19 February 2021, the European Commission finally published two draft adequacy decisions, including one governing private sector data flows, thereby launching[116] the adoption procedures. In its draft decision, the Commission considers that the UK standard of data protection is essentially equivalent to EU standards. To maintain separate strands of analysis, the following sections will first discuss concerns regarding UK data adequacy and subsequently analyse the relevant draft decision.

4.1. Doubts regarding UK data adequacy

Although an adequacy decision is in the mutual interest of the parties and the cost of inadequacy is high,[117] the UK's legislative framework and data-related practices may preclude an adequacy decision, as they may not provide for a level of data protection that is essentially equivalent to that of the EU. Privacy professionals, academics, supervisory authorities and civil society organisations[118] have raised concerns regarding, inter alia,[119] the aspects discussed below.

---

[114] Massé E., Access Now's memo on the data transfers and PNR provisions under the EU-UK Trade Agreement, accessnow, 15 January 2021, p. 1.

[115] Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, European Data Protection Supervisor, 22 February 2021.

[116] International dimension of data protection > Brexit, European Commission website.

[117] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020; D. Castro and E. Chivot, Not granting GDPR adequacy to the UK would be a mistake, Privacy Perspectives, IAPP, 14 September 2020; O. Patel and N. Lea, EU-UK Data Flows, Brexit and No Deal: Adequacy or Disarray?, UCL European Institute, August 2019.

[118] For an in-depth analysis see D. Korff and I. Brown, The inadequacy of UK data protection law: Executive Summary / Part 1: General inadequacy / Part 2: UK surveillance, Data protection and digital competition blog, 9 October-30 November 2020; O. Patel and N. Lea, EU-UK Data Flows, Brexit and No Deal: Adequacy or Disarray?, UCL European Institute, August 2019; D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021; O. Patel, Written evidence (PBS0029), UK Parliament, June 2020; G. Kon and R. Cumbley, EU: Data flows post-Brexit - Choppy waters ahead?, Linklaters, 2 November 2020; C. Pounder, An adequacy determination does not resolve the lower standard of data protection in the UK, Hawktalk blog, 19 November 2020; C. Pounder, Draft Brexit Data Protection Regulations would undermine adequacy determination for the UK, Hawktalk blog, 18 January 2019; G. Smith, Hard questions about soft limits, Cyberleagle blog, 15 October 2020; G. Smith, What will be in Investigatory Powers Act Version 1.2?, Cyberleagle blog, 30 October 2018.

[119] Additional concerns were raised, for instance, as regards the independence of the UK data supervisory authority (Recital 85-91 draft adequacy decision), the UK's wavering commitment to the Convention on Human rights (Recitals 7-10 draft adequacy decision), and broadly-phrased warrants as well as marginal scrutiny of warrants. See also D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021.

4.1.1. UK surveillance laws and practices

According to a recent in-depth analysis,[120] UK surveillance activities do not comply with EU data protection and privacy standards. In particular, academics argue that the UK Government Communications Headquarters (GCHQ) intercepts, retains and analyses masses of personal data, inter alia, by collaborating with or compelling private actors to provide access points, in submarine communication cables for instance. While all data flowing past a given access point is screened indiscriminately, it is uncertain how much of the data is temporarily retained or intercepted for triage, or forwarded to headquarters for analysis. Experts consider that reports are obfuscated, but that it is likely that all metadata is extracted, while content data is preselected to discard 'traffic that takes up a lot of space but has low intelligence value, such as consumer videos and file-sharing media downloads'.[121] The data is used to investigate the communications of individuals already 'known' to pose a threat or to generate new intelligence leads, i.e. previously unknown persons 'of interest'. Experts[122] strongly suspect that big data mining technologies and automated, as well as AI-based processing, are deployed[123] to, for instance, identify individuals as possible or probable terrorists. Such algorithmic detection, however, entails three main problems, namely the mathematically unavoidable fact of a large number of false positives or false negatives when searching for rare instances in large data sets ('base-rate fallacy'),[124] built-in biases[125] and opaque processing (the 'black box phenomenon'). According to the aforementioned experts,[126] these intelligence activities conflict with EU data protection standards developed in numerous CJEU[127] and European Court of Human Rights (ECtHR)[128] cases, as well as with EDPB recommendations[129] on the 'European Essential Guarantees for surveillance measures'. The mandatory retention of data imposed on network providers and subsequent access and extraction of data (including metadata) by intelligence agencies present separate instances of interference with individuals' fundamental rights. Such interferences must be based on 'law', limited to what is strictly 'necessary', and

[120] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020; The analysis draws on, for instance, the report on Privacy and Security: A modern and transparent legal framework, UK, 12 March 2015, of the Parliament's Intelligence and Security Committee (ISC) as well as on the report Collect it all: GCHQ and mass surveillance, Open Rights Group, 3 November 2015, by J. Ruiz et al. See also the UK Government's response to the ISC report [restricted access].

[121] Ruiz J. et al., Collect it all: GCHQ and mass surveillance, Report, Open Rights Group, 3 November 2015, p. 13.

[122] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, pp. 20-24 and pp. 47-48.

[123] H. Warrell, UK spy agency to use AI against cyber attacks and state actors, *Financial Times*, 24 February 2021.

[124] B. Schneier, Data Mining for Terrorists, Schneier on Security blog, 9 March 2006.

[125] D. Barnard-Wills, Review of Gandy's Coming to Terms with Chance, *Surveillance & Society*, Vol. 8(3), 2011, pp. 379-381.

[126] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, pp. 28-29.

[127] For instance: Judgement in Joined Cases C-293/12 and C-594/12 – *DRI*, CJEU, 8 April 2014; judgment in Joined Cases C-203/15 and C-698/15 – *Tele2/Watson*, CJEU, 21 December 2016; judgment in Case C-362/14 – *Schrems I*, CJEU, 6 October 2015; judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020; judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and others*, CJEU, 6 October 2020; judgment in Case C-623/17 – *Privacy International*, CJEU, 6 October 2020.

[128] For instance: judgement in Case with application no 5029/71 – *Klaas*, ECtHR, 6 September 1978; judgment in Case with application no 8691/79 – Malone, ECtHR, 2 August 1984; decision on admissibility of application no 54934/00 – *Weber and Saravia*, ECtHR, 29 June 2006; judgment in Case with application no. 58243/00 – *Liberty*, ECtHR, 1 July 2008; judgment in Case with application no. 26839/05 – Kennedy, ECtHR, 18 May 2010; judgment in Case with application no 47143/06 – *Zakharov*, ECtHR, 4 December 2015; judgment in Joined Cases with a applications nos 58170/13, 62322/14 and 24960/15 – *Big Brother Watch and others*, ECtHR, 4 February 2019 (referral to the Grand Chamber on 4 February 2019, see hearing); see also Factsheet - Mass surveillance, ECtHR, October 2020.

[129] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board, 10 November 2020.

'proportionate' to the respective 'legitimate' intelligence purpose. Since the Investigatory Powers Act 2016 (IPA)[130] presents the legal basis and only provides for safeguards and 'oversight of broad discretionary powers', some[131] argue that it conflicts with the CJEU[132] requirement that the legal basis must itself define the scope of the limitation on fundamental rights and freedoms. In other words, while the CJEU case law trends towards requiring hard limits, UK laws contain soft limits. Additionally, 'the UK IPA rules that allow for the extraction, in bulk, of at least all the metadata of all communication that flow through' access points, are considered[133] incompatible with the CJEU's strict limitation[134] of indiscriminate **retention** as well as **analysis** to 'serious', 'genuine and present or foreseeable' threat to 'the essential functions of the State and fundamental interests of society', as well as the CJEU's limitation[135] of **access** by and **transmission** to intelligence agencies to what is strictly necessary. Additionally, the oversight requirements in the Investigatory Powers Act do not explicitly address the rules for oversight of modern analytical processing (e.g. AI-based). Consequently, this may not satisfy the CJEU's requirement[136] for an effective oversight system that verifies that 'the conditions and safeguards which must be laid down are observed'.[137] Moreover, the IPA does not require the Investigatory Powers Commissioner to disclose intrusive data processing to the data subject, even where it would not jeopardise intelligence activities. This contravenes[138] the notification requirement as stipulated by the ECtHR,[139] the CJEU[140] and the EDPB.[141] Some experts conclude[142] that the UK legal framework does not present meaningful protection against undue access and processing of data for surveillance purposes and thereby does not ensure an essentially equivalent level of data protection.

4.1.2. Shortcomings in the implementation of EU data protection standards

Concerns[143] have also been raised as regards the processing of personal data for immigration purposes ('immigration exemption').[144] As set out in two European Parliament resolutions from

[130] Investigatory Powers Act 2016.

[131] G. Smith, Hard questions about soft limits, Cyberleagle blog, 15 October 2020.

[132] Judgement in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020.

[133] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, pp. 41.

[134] Judgement in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and others*, CJEU, 6 October 2020.

[135] Judgement in Case C-623/17 – *Privacy International*, CJEU, 6 October 2020.

[136] Judgement in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and others*, CJEU, 6 October 2020.

[137] G. Smith, What will be in Investigatory Powers Act Version 1.2?, Cyberleagle blog, 30 October 2018; D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, pp. 42-43.

[138] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, p. 44.

[139] Judgement in Case with application no. 47143/06 – *Zakharov*, ECtHR, 4 December 2015.

[140] Judgement in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and others*, CJEU, 6 October 2020.

[141] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board, 10 November 2020.

[142] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020.

[143] O. Patel and N. Lea, EU-UK Data Flows, Brexit and No Deal: Adequacy or Disarray?, UCL European Institute, August 2019, p. 11; D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020, pp. 17-19.

[144] Immigration exemption, Information Commissioner's Office website.

February[145] and June 2020,[146] the 'UK Data Protection Act provides for a general and broad exemption from the data protection principles and data subjects' rights for the processing of personal data for immigration purposes'. However, these only apply where giving effect to data subjects' rights would jeopardise 'effective immigration control' or the 'investigation or detection of activities that would undermine the maintenance of effective immigration control'. This exemption allows, for instance, the undisclosed processing of data and the refusal of access requests where disclosure would prejudice immigration control. Civil rights organisations have challenged[147] this provision in court, based on the argument that it is too vague and broad and has allowed for arbitrary denial of data subjects' rights. While the UK High Court held[148] that the provision applies to a sufficiently narrow and clear range of situations, the applicants seek[149] to appeal the 2019 immigration exemption judgment. In a recent submission[150] to the European Commission concerning the draft adequacy decision, one of the applicant organisations in this case claimed and evidenced the excessive practical application of the exemption and concluded an incompatibility with EU data protection standards. Additionally, concerns have been raised[151] that the Digital Economy Act 2017[152] (DEA) may excessively liberalise public sector sharing of data that does not reveal the identity of – yet serves to single out – an individual. The pertinent DEA provisions would therefore fail to afford data subjects an equivalent level of protection, unless the caveat that nothing in the respective provisions may 'contravene the data protection legislation' is strictly applied.

4.1.3. Weak UK enforcement of data protection rules

One civil society organisation[153] pointedly questions the effective functioning of the UK data protection supervisory authority[154] (ICO). The ICO has also recently been criticised[155] by some UK Members of Parliament for failing to protect peoples' rights. Commentators have remarked multiple instances[156] of enforcement failures and drawn up unsettling statistics[157] (hard enforcement in less than 0.025 % of cases). With a view to limited enforcement[158] across the EU, some privacy

[145] Resolution on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland, European Parliament, 12 February 2020, para. 32.

[146] Resolution on recommendations on the negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland, European Parliament, 18 June 2020, para. 80.

[147] M. Rice, What is at stake with the immigration exemption legal challenge?, Open Rights Group blog, 3 August 2018.

[148] Judgement in Case No. CO/3386/2018, UK High Court of Justice, 3 October 2019.

[149] Open Rights Group and The3million seek to appeal immigration exemption judgement, press release, Open Rights Group, 3 October 2019.

[150] The UK's Immigration Exemption in the Data Protection Act 2018 and data adequacy, Submission to the European Commission, Open Rights Group, 2 March 2021.

[151] D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020, pp. 16-17.

[152] Digital Economy Act 2017.

[153] The Commission's obligation to refuse an "adequacy decision" to the United Kingdom due to inadequacy of enforcement of personal data protection in that jurisdiction, Irish Council of Civil Liberties, 12 October 2020.

[154] Enforcement action, Information Commissioner's Office website.

[155] M. Burgess, MPs slam UK data regulator for failing to protect people's rights, WIRED, 21 August 2020.

[156] L. Woods, Data Protection, the UK and the EU: the draft adequacy decisions, EU Law Analysis blog, 24 February 2021.

[157] D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021, pp. 22-24.

[158] Resolution on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, European Parliament, 25 March 2021, para. 12-18; Resolution Massé E., Two years under the EU GDPR: An implementation progress report, accessnow, May 2020; In opposition to the criticism in the Draft motion for a resolution on Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") - Case C-311/18, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 13 January 2021, para. 3, the

professionals[159] consider that this should not constitute a barrier to a positive adequacy decision from the Commission.

4.1.4. Potential liberal onward transfer of data

Article 44 GDPR expressly states that the GDPR transfer conditions also apply to the onward transfer of personal data to a third country outside the UK and that such an onward transfer should not undermine the level of protection guaranteed by the GDPR. A primary data recipient may only transfer[160] personal data onwards, 'where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision.'

Current and predicted UK legal regimes raise particular concerns[161] regarding compliance with Article 44 GDPR:

(i) Allegedly, the data sharing arrangements between the 'Five Eyes'[162] intelligence alliance (United States of America, UK, Australia, Canada and New Zealand) provides[163] for the full exchange of intelligence by default and involves the onward transfer of data from the UK to the USA – a country whose level of data protection has been deemed[164] inadequate by the CJEU.

(ii) The EDPB has doubts[165] regarding whether remote computing services under the jurisdiction of the USA might be required to disclose data located in the UK on the grounds of the UK-US Cloud Act Agreement[166] and whether EU data subjects are afforded sufficient safeguards. Members of the European Parliament raised[167] the question of the implications for a UK adequacy decision with the Commission as early as 2019.

Irish Commissioner for Data Protection, Helen Dixon, shines a light on the challenges DPAs face in her Correspondence with the LIBE Committee, 12 March 2020, p. 3-5.

[159] G. Kon and R. Cumbley, EU: Data flows post-Brexit - Choppy waters ahead?, Linklaters, 2 November 2020.

[160] Adequacy Referential, WP 254 rev.01, Article 29 Data Protection Working Party, 6 February 2018, p. 6.

[161] D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020, pp. 8-13.

[162] S. Kim and P. Perlin, Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance, Lawfare, 25 March 2019.

[163] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, p. 25.

[164] Judgment in Case C-311/18 – *Schrems II*, CJEU, 16 July 2020; H. Mildebrath, The CJEU judgment in the *Schrems II* case, At a glance, EPRS, European Parliament, September 2020.

[165] Letters to MEPs on US CLOUD Act and UK-US CLOUD Act Agreement, European Data Protection Board, 15 June 2020.

[166] According to Article 3 of the agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime in conjunction with Section 3 of the US CLOUD Act. For context see T. Christakis, 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts), European Law Blog, 17 October 2019.

[167] UK-US agreement under the US CLOUD Act, Question for written answer E-003136-19, Moritz Körner (Renew, Germany) and Sophia in 't Veld (Renew, Netherlands).

(iii) Certain commentators[168] believe that the UK may significantly liberalise regulation around data flows with the USA, for instance, by means of trade provisions or by a US adequacy decision under its domestic replication of the GDPR ('UK GDPR').

(iv) In the same vein, the UK announced that it will allow[169] transfers to Gibraltar to continue, although the EU has never issued an adequacy decision[170] and the GCHQ intelligence powers equally apply to the British Islands.

(v) Finally, concerns have been raised[171] regarding the UK–Japan Comprehensive Economic Partnership Agreement (CEPA), which may contravene the EU and UK data protection framework. However, it should be noted[172] that the EU has granted Japan an adequacy decision[173] and that Japan has extended[174] the supplementary safeguards therein to its relationship with the UK, notably the 'handling of personal data received from the United Kingdom based on an adequacy decision after the United Kingdom left the EU'.

4.1.5. Wavering commitment to EU data protection standards

Another point of concern arises from the UK's inconsistent position[175] as to whether it will adjust its national legislation to diverge (further) from EU GDPR standards. Prime Minister Boris Johnson stated[176] that 'The UK will in future develop separate and independent policies in areas such as [...] data protection, maintaining high standards as we do so'. A former senior adviser, Dominic Cummings, championed[177] a radical 'pro-tech' plan and intended to 'rewrite Britain's data protection laws'. As evidenced by the 2020 National Data Strategy[178], the UK is set to follow 'an ambitious, pro-growth strategy that aims to drive the UK in building a world-leading data economy while ensuring public trust in data use'. Most recently, UK Culture Secretary Oliver Dowden reportedly stated that the UK could 'apply drive to getting a more expansive and more rapid data adequacy agreement with third countries in a way that will open up data opportunities',[179] now that it has withdrawn from the EU.

[168] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020, p. 10-11; D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020, p. 12.

[169] International data transfers, Information Commissioner's Office website.

[170] Section I1: Gibraltar's Legislative Framework and Alignment with the UK, Explanatory framework for adequacy discussions, Policy papers, UK Government, 13 March 2020.

[171] J. Ruiz, What the UK-Japan trade deal means for digital rights, Briefing, Open Rights Group, 5 November 2020.

[172] M. Lachenmann, Data transfers between the EU and Japan: an introduction to the EU's adequacy decision on Japan, LinkedIn, 2 July 2019.

[173] Adequacy decisions, European Commission website.

[174] Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision, Personal Information Protection Commission Japan.

[175] M. Scott and V. Manancout, What you need to know about EU, US and UK data talks, Politico, 2 November 2020.

[176] UK / EU relations, Statement UIN HCWS86, Prime Minister Boris Johnson, 3 February 2020.

[177] D. Boffey, Dominic Cummings' data law shake-up a danger to trade, says EU, *The Guardian*, 25 September 2020

[178] UK National Data Strategy, Policy paper, UK Government Department for Digital, Culture, Media & Sport, 9 September 2020.

[179] A. Dickson, Dowden: UK will diverge from 'protectionist' EU on data, Politico Pro, 11 March 2011.

The European Parliament's LIBE committee recently reinforced these concerns, expressing its view[180] that:

- 'the UK legal framework on retention of electronic telecommunications data does not fulfil the condition of the relevant EU *acquis*' and
- that the Commission should scrutinise 'international agreements of the UK on personal data transfers', as well as
- the UK legal framework 'in the fields of national security and for the processing of personal data by law enforcement authorities'.

Subsequently, the committee 'calls on the Commission to ensure that the UK has resolved the problems identified in its opinion prior to considering UK data protection law adequate in line with Union law as interpreted by the Court of Justice'. As remedial action, commentators suggest[181] that the EU should withhold a positive adequacy decision until the UK, for instance:

- aligns the definition of 'personal data' in the UK Digital Economy Act[182] with the respective definition in the GDPR,
- tightens the immigration exemption in the Data Protection Act 2018[183] and applies it in a more clear and foreseeable manner,
- assures that it will not significantly diverge from EU data protection standards,
- agrees to provisions that prevent it from undermining the afforded level of protection through onward transfers, for instance by restricting the free flow of personal data to those countries that have been issued adequacy by the EU,[184]
- strongly assures that its supervisory authority will enforce data subjects' rights,
- commits to a revision of its surveillance laws and practices.

Conversely, technology and security advocates, as well as business-friendly commentators, encourage[185] the Commission to grant a positive adequacy decision for the following reasons:

- The EU might disrupt data flows to one of the leading countries in artificial intelligence, leading to the Union falling further behind in the digital economy,
- suggesting that the UK is not adequate would 'set the bar for adequacy impossibly high',[186] since the UK has already shown its adherence to the GDPR as a Union member and a national replication of the GDPR remains in place post-Brexit ('UK GDPR'),
- the export of data protection standards ('Brussels effect'),[187] hurts EU competitiveness,[188]

[180] Opinion on the Trade and Cooperation Agreement, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 5 February 2021, p. 5.

[181] D. Korff and I. Brown, The inadequacy of UK data protection law: Executive Summary, Data protection and digital competition blog, 30 November 2020.

[182] Digital Economy Act.

[183] Data Protection Act 2018.

[184] In the course of adopting a domestic replication of the GDPR ('UK GDPR'), the UK also introduced a national adequacy mechanism essentially providing for the (formal) continuity of protection. This may be undermined by, for instance, concluding trade agreements equipped with primacy over the UK's domestic adequacy mechanism.

[185] D. Castro and E. Chivot, Not granting GDPR adequacy to the UK would be a mistake, Privacy Perspectives, IAPP, 14 September 2020.

[186] E. Duhs, EU-UK data flows, adequacy and regulatory changes from 1st January 2021, LinkedIn, 28 December 2020.

[187] A. Beattie, The Brussels Effect, by Anu Bradford, *Financial Times*, 27 January 2020.

[188] E. Chivot and D. Castro, The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy, Center for Data Innovation, 13 May 2019.

- the extraterritorial disciplinary effect of the GDPR might[189] prevent effective protection against military action,
- the EU scrutiny of foreign intelligence measures may have a 'flavour of differential treatment'[190] or even 'hypocrisy and double standards'[191], given that Member States do not meet[192] CJEU standards and the CJEU is precluded from scrutinising Member States' national intelligence measures pursuant to Article 4(2) TEU. However, the CJEU has recently narrowed[193] the applicability of this exemption in its judgment 'Privacy International',[194] which may lead to a rapprochement[195] of the standards applicable to Member States and third countries. Additionally, CJEU Judge Thomas von Danwitz, holds that this discrepancy simply reflects the division of competences as well as the explicit requirements in Article 45 GDPR.[196]

It should also be noted that it is uncertain to what extent EU intelligence agencies still[197] benefit from collaboration with UK agencies, including data sharing, and to what extent denying an adequacy decision would safeguard EU data from UK surveillance. While the arguments in favour of an adequacy decision present valid concerns, they partially assume that the EU's notion of data protection and CJEU judgments are fundamentally flawed. Only recently, CJEU Judge Thomas von Danwitz emphasised that the fundamental decision in favour of a high level of data protection also extends to data transfer provisions, even where this entails adverse economic effects.[198] Nevertheless, these concerns certainly shine a light on the economic ramifications and controversies surrounding the potential refusal of an adequacy decision. Considering the broad economic, privacy and security implications, as well as the sharp divide among stakeholders, any decision by the Commission would inspire mixed reviews.

4.2. European Commission draft adequacy decision in context

On 19 February 2021, the Commission launched[199] the procedure for the adoption of two adequacy decisions for transfers of personal data to the UK, under the GDPR and the Law Enforcement Directive (LED) respectively. With the publication of its draft adequacy decision, the Commission began the process of adopting an adequacy decision that enables the commercial transfer of personal data without the need to obtain any further authorisation (see Box 1 – Procedure for

[189] P. Swire, 'Schrems II' backs the European legal regime into a corner — How can it get out?, IAPP Privacy Perspectives, 16 July 2020.

[190] K. Irion, Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law, European Law Blog, 24 July 2020.

[191] D. Korff and I. Brown, The inadequacy of UK data protection law: Executive Summary, Data protection and digital competition blog, 30 November 2020, p. 10.

[192] D. Korff et al., Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, University of Cambridge Faculty of Law Research Paper No. 16/2017, March 2017; Kelber U. (Federal Commissioner for Data Protection and Freedom of Information of Germany), Aspects where Germany's draft Federal Intelligence Services Act misses the mark, about:intel, 16 February 2021.

[193] J. Sajfert, Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy, European Law Blog, 26 October 2020.

[194] Judgement in Case C-623/17 – *Privacy International*, CJEU, 6 October 2020.

[195] K. Propp, Putting privacy limits on national security mass surveillance: The European Court of Justice intervenes, Atlantic Council, 21 February 2020.

[196] CJEU Judge von Danwitz T., European Data Protection Day 2021, 28 January 2020, 2:50:28-2:52:53.

[197] Hosenball M., British spy agencies see foreign ties intact despite Brexit, Reuters, 12 August 2019.

[198] CJEU Judge von Danwitz T., European Data Protection Day 2021, 28 January 2020, 1:12:10-1:12:43, 1:30:07-1:31:55, 2:18:01-2:19:27, 2:46:02-2:47:57 (for details cf. section '5. Conclusion').

[199] International dimension of data protection > Brexit, European Commission website.

adopting adequacy decisions). The draft decision contains a comprehensive analysis of the UK's privacy-related legal regime and attempts to dispel concerns raised by experts (see section 'Doubts regarding UK data adequacy' above).

4.2.1. UK surveillance laws and practices

In Recitals 112-265 of the draft adequacy decision, the Commission assess the UK's legal framework for the collection and subsequent use of personal data by UK public authorities, including intelligence agencies, notably for criminal law enforcement and national security purposes. It mentions particularly relevant case law in Recitals 114-115 and selectively highlights similarities with the EU legal regime throughout the text. The section is subdivided into type of investigatory power and whether the power is exercised on a specific target or in bulk. As regards privacy and security, the Commission factors in limitations and safeguards such as: (i) the requirement to obtain a warrant or production order, including following a 'double-lock' procedure and an information-based assessment; (ii) limits on the duration, renewal and modification of warrants; (iii) the conditions of necessity and proportionality, both as regards operational objectives and technical options; (iv) additional limitations and safeguards relating to communications of persons with a specific status, e.g. Members of Parliament; (v) storage, erasure and disclosure conditions concerning collected data; (vi) limiting processing activities to statutorily mandated cases; (vii) ex-post oversight in cases of urgent data processing. Finally, the Commission holds that data subjects enjoy effective administrative and judicial redress rights, including the possibility to obtain access to their data or rectification or erasure of such data. Ultimately, the Commission considers that concerns[200] raised, inter alia, by the Snowden revelations and the UK 2015 report on Privacy and Security,[201] have been sufficiently dispelled by the reform of the Regulation of Investigatory Powers Act 2000, culminating in the IPA 2016 (footnote 465 of the draft adequacy decision). This reform was also welcomed by UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, who stated,[202] that 'While the new set-up may still contain a number of imperfections, the UK has now equipped itself with a legal framework and significant resources designed to protect privacy without compromising security'. As bulk powers remain very controversial, one way forward might be to analyse whether the UK legal framework and surveillance practices meet the requirements of EU case law[203] and clarify how intelligence agencies may leverage bulk investigatory powers for law enforcement purposes.

4.2.2. Shortcomings in the implementation of EU data protection standards

In line with a UK High Court decision,[204] the Commission considers that the immigration exemption is sufficiently narrow and does not excessively curtail data subjects' rights (Recitals 62-65). A thorough reinvestigation of the immigration exemption may address concerns repeatedly raised by

[200] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020.

[201] Privacy and Security: A modern and transparent legal framework, UK Parliament's Intelligence and Security Committee (ISC), 12 March 2015; UK Government's response to the ISC report [restricted access].

[202] End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the UK and Northern Ireland, Joseph Cannataci, 29 June 2018.

[203] Notably the conditions stipulated in the judgement in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and others*, CJEU, 6 October 2020 (cf. section '4.1.1 UK surveillance laws and practices'). For more relevant case law see D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, pp. 28-29 and Opinion on the Trade and Cooperation Agreement, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 5 February 2021, para. 13, fn. 6 as well as Factsheet - Mass surveillance, ECtHR, October 2020.

[204] Judgment in Case No. CO/3386/2018, UK High Court of Justice, 3 October 2019.

the European Parliament[205] and the Open Rights Group.[206] Similarly, the Commission holds that public-sector data sharing, under the Digital Economy Act 2017,[207] notably between law enforcement authorities and other authorities, provides for compliance with the principles in the Data Protection Act 2018, which contain sufficient safeguards (Recitals 142-143).

4.2.3. Weak UK enforcement of data protection rules

The Commission highlights the UK ICO's enforcement powers, as well as cases of due enforcement (Recitals 92-98). However, in light of the ICO's unsettling enforcement statistics,[208] a mitigation strategy, such as requesting assurances from the UK that its supervisory authority will give **adequate** effect to the UK data protection *acquis*, is arguably required.

4.2.4. Potential liberal onward transfer of data

Instead of explicitly addressing concerns[209] over UK trade and adequacy arrangements with third countries that may bypass adequacy, the Commission holds that the 'level of protection [...] must not be undermined by the further transfer of [...] data to recipients in a third country' and that the retained GDPR transfer mechanisms in UK law provide for the 'continuity of protection' (Recital 75-82). The Commission relies on standard EU adequacy provisions, including monitoring and suspension mechanisms, to deter the UK from bypassing adequacy in trade and adequacy arrangements. The Commission also addresses concerns[210] that US authorities may compel providers to share EU data based on the US Cloud Act[211] in conjunction with the UK-US Cloud Act Agreement[212], without satisfying essential, but inapplicable, safeguards. In Recitals 151-154, the Commission attempts to dispel these concerns on the grounds that safeguards enshrined in the UK-US Cloud Act Agreement apply and that EU data will benefit from the EU-US Umbrella Agreement[213] – a comprehensive data protection agreement in the area of law enforcement cooperation. However, the Commission does not precisely clarify the interplay[214] between UK-US Cloud Act Agreement and US domestic law provisions and it does not define and assess the specific safeguards of the UK-US Cloud Act Agreement. While the Commission acknowledges that 'the details of the concrete implementation of the data protection safeguards are still subject to discussions between the UK and the US', it attempts[215] to reassure by emphasising that it will pay particular attention to

[205] Resolution on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland, European Parliament, 12 February 2020, para. 32; Resolution on recommendations on the negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland, European Parliament, 18 June 2020, para. 80; Opinion on the Trade and Cooperation Agreement, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 5 February 2021, para 10-11.

[206] The UK's Immigration Exemption in the Data Protection Act 2018 and data adequacy, Submission to the European Commission, Open Rights Group, 2 March 2021.

[207] Digital Economy Act 2017.

[208] D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021, pp. 22-24.

[209] D. McCann et al., The cost of data inadequacy, New Economics Foundation, 23 November 2020, p. 10-11; D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020, p. 12.

[210] Letters to MEPs on US CLOUD Act and UK-US CLOUD Act Agreement, European Data Protection Board, 15 June 2020.

[211] US Cloud Act.

[212] UK-US Cloud Act Agreement.

[213] EU-US Umbrella Agreement.

[214] T. Christakis and K. Propp, The legal nature of the UK-US Cloud Agreement, Cross-Border Data Forum, 20 April 2020.

[215] D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021.

the application and adaptation of the Umbrella Agreement's protections to UK-US transfers under the UK-US Cloud Act Agreement. One approach to dispel critique might be to clarify the precise interplay[216] between provisions in the UK-US Cloud Act Agreement and US domestic law and gauge identified safeguards against EU case law. Data sharing between UK and third-country intelligence agencies are considered adequate upon general reference to safeguards in Section 109 DPA 2018[217] and provisions of the IPA 2016 (Recitals 236-237). With a view to alleged[218] liberal data sharing among the 'Five Eyes'[219] and concerns[220] regarding intelligence sharing in general, the relevant provisions might merit an in-depth assessment.

4.2.5. Wavering commitment to EU data protection standards

The European Commission does not address this concern explicitly, but emphasises that monitoring is particularly important as the UK 'will administer, apply and enforce a new data protection regime' (Recitals 274-280). Under the pretext of the UK's introduction of a new data protection framework, the Commission intends to restrict the validity of the adequacy decision to four years (Recitals 281-282). While the Commission always holds the power to repeal, amend or suspend the decision if it considers that a third country no longer ensures an adequate level of protection (Article 45(5) GDPR), this is the first time that the Commission has proposed an expiration date for its adequacy decision, a 'sunset clause'. European Commissioner for Justice, Didier Reynders, explained in his presentation[221] of 16 March 2021 made to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs that after four years, the entire adequacy decision procedure, including an opinion from the EDPB and obtaining approval from the Member States in the comitology procedure, would need to be reiterated. The Commission proposes four years, as 'it will take some time before the UK's approach to data protection will be fully developed. [The European Commission] can only decide whether the adequacy decision should be renewed, once [it] know[s] in which direction the UK is moving and [has] some good understanding and experience on how the fully autonomous UK regime will be working in practice.'[222] One commentator[223] considers that this sunset clause 'may reflect concerns regarding the UK government's plans for data protection in the future'.

[216] T. Christakis and K. Propp, The legal nature of the UK-US Cloud Agreement, Cross-Border Data Forum, 20 April 2020.

[217] Section 109 DPA 2018.

[218] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020, p. 25.

[219] S. Kim and P. Perlin, Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance, Lawfare, 25 March 2019.

[220] Bowcott O., UK spy agencies may be circumventing data-sharing law, tribunal told, *The Guardian*, 17 October 2017.

[221] Commissioner for Justice, Didier Reynders, Presentation of two draft implementing decisions by the Commission pursuant to Regulation (EU)2016/679 and Directive (EU)2016/680 on the adequate protection of personal data by the United Kingdom, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 16 March 2021, 10:48:00-11:00:07 and answers to follow-up questions 11:16:47-11:33:07 as well as 11:34:00-11:35:17.

[222] Commissioner for Justice Didier Reynders, Presentation of two draft implementing decisions by the Commission pursuant to Regulation (EU)2016/679 and Directive (EU)2016/680 on the adequate protection of personal data by the United Kingdom, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 16 March 2021, 11:17:30-11:19:23.

[223] Woods L., Data Protection, the UK and the EU: the draft adequacy decisions, EU Law Analysis, 24 February 2021.

Table 2 – Adequacy concerns and the European Commission draft adequacy decision

Adequacy concerns	Suggested remedial action	European Commission approach	Initial assessment
UK security law and intrusive surveillance practices possibly fall short of EU data protection standards	The UK commits to a revision of its surveillance laws and practices	Following an assessment of the limitations and safeguards as well as enforcement mechanisms in Recitals 112-265, the Commission deems the UK's legal framework for the collection and subsequent use of personal data by UK public authorities to be adequate	As bulk powers remain very controversial, one way forward might be to analyse whether the UK legal framework and surveillance practices meet the requirements of EU case law and clarify how intelligence agencies may leverage bulk investigatory powers for law enforcement purposes
Potential deficits in the implementation of EU data protection standards, notably where: (i) data subjects' rights are restricted for immigration purposes, and (ii) public authorities may share data liberally based on the Digital Economy Act 2017 (DEA 2017)	(i) Narrow the immigration exemption, (ii) Align the definition of 'personal data' in the DEA 2017 with that of the GDPR	(i) In line with a UK High Court decision, the Commission considers the immigration exemption to be sufficiently narrow (Recitals 62-65). (ii) Inter alia, because the DEA 2017 subjects the data sharing activities in question to data protection rules, the Commission does not see a need for remedial action (Recitals 142-143)	(i) A thorough reinvestigation of the immigration exemption may address European Parliament and civil society organisation concerns, (ii) The Commission has emphasised its monitoring and suspension powers (Recitals 274-280)
Weak enforcement of data protection rules	Provide strong assurance that the UK will enforce data subjects' rights	Apparently, the Commission does not see cause for concern and instead highlights the ICO's enforcement powers and practices (Recitals 92-98).	In light of the ICO's unsettling enforcement statistics, a mitigation strategy, such as requesting assurances from the UK that its supervisory authority will give adequate effect to the UK data protection *acquis*, is arguably required
Potential liberal onward transfer of data from the UK to third countries lacking adequacy, based on (i) (future) UK commitments to the free flow of data, (ii) the UK-US Cloud Act Agreement, granting US authorities access to data held by UK providers, or (iii) arrangements among the Five Eyes intelligence alliance	(i) Restrict the free flow of data to countries that have been issued an adequacy decision by the EU, (ii) + (iii) the UK commits to a revision of its surveillance laws and practices, including amending its intelligence data sharing agreement	(i) The Commission relies on standard EU adequacy provisions, including suspension mechanisms, to deter the UK from bypassing adequacy requirements in trade and adequacy arrangements (Recital 75-82). (ii) The Commission attempts to dispel concerns over the UK-US Cloud Act Agreement, notably on the grounds that EU data will likely benefit from the EU-US Umbrella Agreement and that its implementation will be monitored (Recitals 151-154). (iii) Similarly, data exchanges between UK and third-country intelligence agencies are considered adequate, with general reference to data protection rules (Recitals 236-237)	(i) The Commission has emphasised its monitoring and suspension powers (Recitals 274-280) (ii) One approach to better safeguard citizens might be to clarify the precise interplay between provisions in the UK-US Cloud Act Agreement and US domestic law and gauge identified safeguards against EU case law, (iii) With a view to alleged liberal data sharing among the Five Eyes alliance and concerns regarding intelligence sharing in general, the relevant provisions might merit an in-depth assessment
Wavering commitment to EU data protection standards post-Brexit	Provide assurance that the UK will not significantly diverge from the EU data protection standards	The Commission does not address the concern explicitly, but emphasises that monitoring is particularly important as the UK 'will administer, apply and enforce a new data protection regime' (Recitals 274-280)	The Commission has emphasised its monitoring and suspension powers (Recitals 274-280).

Source: EPRS, authors' own elaboration based on sources cited in the text above.

5. Conclusion

Ultimately, even the European Data Protection Supervisor appears willing[224] to accept the interim solution, as long as it is not repeated, much less becomes the norm. As a follow-up arrangement to the interim solution, which expires on 30 June 2021, the European Commission launched[225] the process of adopting an adequacy decision on 19 February 2021. While the Commission has a strong position in the adequacy proceedings and, formally, Member States can only stop an intended adoption with a qualified majority (see Article 5(3), sentence 1, Regulation (EU) No 182/2011[226]), all stakeholders have a vested interest in producing a sustainable result that would withstand a challenge before the CJEU; not least because a defeat in court, would erode confidence in this transfer mechanism and strategic complaints are not unlikely.

In its draft adequacy decision, the Commission relies on a UK/EU comparative analysis of statutes, guidance documents and informal bilateral commitments for its assessment of the UK's level of data protection. Presumably, it sets out from the premise that UK authorities, in principle, act in a lawful manner, that former surveillance practices have been brought into accordance with UK law and that potential future deviations and violations are not yet sufficiently manifest as to preclude an adequacy decision. As a mitigating strategy, the Commission emphasises its suspension and termination rights in case inadequacy is revealed and includes an expiration date in the draft decision. Critics consider that the UK level of data protection is not adequate and advocate that certain conditions must be met before granting an adequacy decision. Most prominently, they raise concerns as regards (i) UK surveillance laws[227] and practices,[228] (ii) shortcomings in the implementation of EU data protection standards linked to the immigration exemption[229] and the Digital Economy Act 2017,[230] (iii) weak enforcement[231] of data protection rules by the Information Commissioner's Office (ICO), (iv) potential liberal onward transfer[232] of data, and (v) the UK's wavering commitment[233] to EU data protection standards. One way forward may be a **thorough assessment** of the UK legal framework **against EU standards, including CJEU case law**. Where risk of non-compliance is low and legal remedies are likely effective, commitments to a specific interpretation of the law as well as assurances of compliance might suffice as a mitigation strategy. Where serious doubts regarding UK data adequacy persist, supplementary rules, including additional safeguards, could be agreed and included in the adequacy decision, to bridge the differences between the two data protection systems. To promote mutual understanding and foster sustainable cooperation, the parties may consider further aligning visions and expectations, for

[224] Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, European Data Protection Supervisor, 22 February 2021.

[225] International dimension of data protection > Brexit, European Commission website.

[226] Regulation (EU) No 182/2011.

[227] G. Smith, Hard questions about soft limits, Cyberleagle blog, 15 October 2020.

[228] D. Korff and I. Brown, The inadequacy of UK data protection law Pt 2: UK surveillance laws, Data protection and digital competition blog, 30 November 2020.

[229] The UK's Immigration Exemption in the Data Protection Act 2018 and data adequacy, Submission to the European Commission, Open Rights Group, 2 March 2021.

[230] D. Korff and I. Brown, The inadequacy of UK data protection law: Pt 1: General inadequacy, Data protection and digital competition blog, 9 October-30 November 2020.

[231] D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021, pp. 22-24.

[232] Letters to MEPs on US CLOUD Act and UK-US CLOUD Act Agreement, European Data Protection Board, 15 June 2020.

[233] UK / EU relations, Statement UIN HCWS86, Prime Minister Boris Johnson, 3 February 2020.

instance, in the framework of joint governance teams[234], within a specialised TCA committee (Articles INST.1(4)(h) and INST.2(1)(f) TCA[235]) or in multilateral councils and organisations[236]. When assessing the UK level of data protection against EU standards, it is important to keep in mind that CJEU Judge Thomas von Danwitz recently emphasised that the fundamental decision in favour of a high level of data protection extends to data transfer provisions, in spite of adverse economic effects:

> *'Let me just mention in passing that data transfers to third countries are not rare incidents. It is common practice to outsource certain data-based services [...] to third countries. This may be economically useful and desirable for enterprises, but it should not compromise the level of protection ensured in the European Union. The necessary balance between the legitimate interests of economic operators and the promotion of international trade on one hand, and the right to the protection of personal data on the other hand, is reflected in the legal requirement to ensure an essentially equivalent level of protection of personal data. The fact that this level of protection in third countries is not for free or maybe cannot be ensured at all, may have economic disadvantages for companies in individual cases, nevertheless, it is the necessary consequence of the fundamental decision taken in European data protection law to ensure a high level of protection of personal data. To a certain extent, the GDPR thus claims respect of the principle of European data sovereignty. In principle, this boils down to respect for the data sovereignty of the European citizens, which is the goal that the GDPR rightly puts in relation to the Unions fundamental values.'*[237]

Clearly, the UK and the EU are faced with the very delicate task of resolving tensions between economic, privacy, security and autonomy[238] considerations, as well as interrelated fundamental rights in the face of an unrelenting data protection regime. Considering the broad implications, as well as the sharp divide among proponents and opponents, finding a solution will not be easy. In its highly anticipated opinion on the draft decision, scheduled for mid-April,[239] the European Data Protection Board will likely scrutinise the Commission's approach and provide recommendations on

---

[234] While addressing a very different, private sector, scenario, inspiration might be drawn from Frydlinger D. et al., A New Approach to Contracts, *Harvard Business Review*, September-October 2019.

[235] Articles INST.1(4)(h) and INST.2(1)(f) TCA.

[236] S. Lowe and C. Mortera-Martinez, Post-Brexit data transfers are not a done deal, Centre for European Reform, 29 March 2021, argue that the EU might consider opening up membership of its proposed EU-US Trade and Technology Council (TTC) – the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy only recently suggested establishing such a Council in a joint communication from 2 December 2020 on 'A new EU-US agenda for global change', JOIN(2020) 22. T. Barker, Breaking the Transatlantic Data Trilemma, German Council on Foreign Relations, December 2020, advocates a trilateral approach together with the US aimed at determining surveillance thresholds and redress mechanisms as well as a twin-track cooperation with like-minded countries such as Australia, Japan and South Korea on an international level.

[237] CJEU Judge von Danwitz T., European Data Protection Day 2021, 28 January 2020, 1:30:07-1:31:55. Later on (3:10:28-3:10:50) he adds *'I do not like the term data sovereignty; it is more about giving European citizens the opportunity to protect their data, to be sovereigns over their data.'* Previously, he had stated (1:12:10-1:12:43) that *'it is not the task of a Court to find the least problematic solution to a case'* and that (2:18:01-2:19:27) *'In the cases Schrems I and Schrems II [...], the question was always, what is stronger: the economic power of certain enterprises and operators or the legal framework and I always referred to the provisions in the Data Protection Regulation not so much to case law; that's what I meant when I said this judgment was not surprising, because it's all in the legal bases'*. While he is aware that the invalidation of an adequacy decision places heavy burdens on companies, especially SMEs, 'this is what the GDPR demands' (2:46:02-2:47:57).

[238] Due to the extraterritorial disciplinary effect of GDPR provisions on international data transfers, commentators speak of an 'incomplete emancipation' in the area of data protection. While the UK may feel subjected to a certain disciplinary effect, formally speaking, the provisions safeguard an adequate level of protection only for 'personal data of data subjects who are in the Union'. In the words of CJEU Judge Thomas von Danwitz, *'this boils down to respect for the data sovereignty of the European citizens'*.

[239] Commissioner for Justice Didier Reynders, Presentation of two draft implementing decisions by the Commission pursuant to Regulation (EU)2016/679 and Directive (EU)2016/680 on the adequate protection of personal data by the United Kingdom, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 16 March 2021, 10:59:12-11:00:07.

next steps. While the opinion is formally non-binding, it will likely present a litmus test for the draft decision. A first in-depth analysis of the draft decision is already available.[240]

[240] D. Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021; The author, Emeritus Professor D. Korff, already provided a note on European & International Law on Trans-National Surveillance for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in 2013.

6. References

Institutional documents

Adequacy Referential, WP 254 rev.01, Article 29 Data Protection Working Party, 6 February 2018

'Chapter 9: Digital trade and data flows', in *The future UK-EU relationship on professional and business services*, UK Parliament's European Union Committee, 13 October 2020

Factsheet - Mass surveillance, ECtHR, October 2020

Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, European Data Protection Board, 23 July 2020

Using personal data in your business or other organisation, Guidance, UK Government Department for Digital, Culture, Media & Sport, the Department for Business, Energy & Industrial Strategy, and the Information Commissioner's Office, 31 December 2020.

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, European Data Protection Board, 4 June 2019

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, European Data Protection Board, 4 June 2019;

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, European Data Protection Board, 25 May 2018

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), European Data Protection Board, 4 June 2019

Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, European Data Protection Board and European Data Protection Supervisor, 14 January 2021

Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?, DG XV D/5057/97 final, Article 29 Data Protection Working Party, 14 January 1998

Letters to MEPs on US CLOUD Act and UK-US CLOUD Act Agreement, European Data Protection Board, 15 June 2020

Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, European Data Protection Supervisor, 22 February 2021

Privacy and Security: A modern and transparent legal framework, UK Parliament's Intelligence and Security Committee (ISC), 12 March 2015

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Board, 10 November 2020

Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board, 10 November 2020

Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger, press release, Conference of the German Data Protection Authorities (DSK), 28 July 2020

Understanding and measuring cross-border digital trade, UK Department for International Trade and UK Department for Digital, Culture Media & Sport, 14 May 2020

Withdrawal of the United Kingdom and the EU rules in the field of data protection, Notice to stakeholders, European Commission, 6 July 2020

Further reading

101 Complaints on EU-US transfers filed, NOYB website, 17 August 2020

Annual Governance Report 2019, IAPP and EY

Barker T., Breaking the Transatlantic Data Trilemma, German Council on Foreign Relations, December 2020

Barnard-Wills D., Review of Gandy's Coming to Terms with Chance, *Surveillance & Society*, Vol. 8(3), pp. 379-381

Beattie A., The Brussels Effect, by Anu Bradford, *Financial Times*, 27 January 2020

Bergt M., 'Artikel 40 DS-GVO' and 'Artikel 42 DS-GVO', in Kühling J. and Buchner B., *DS-GVO BDSG Kommentar*, C.H.Beck, 2018

Boffey D., Dominic Cummings' data law shake-up a danger to trade, says EU, *The Guardian*, 25 September 2020

Bowcott O., UK spy agencies may be circumventing data-sharing law, tribunal told, *The Guardian*, 17 October 2017

Burgess M., MPs slam UK data regulator for failing to protect people's rights, WIRED, 21 August 2020

Castro D. and Chivot E., Not granting GDPR adequacy to the UK would be a mistake, Privacy Perspectives, IAPP, 14 September 2020

Celeste E., Cross-Border Data Protection After Brexit, Brexit Institute Working Paper Series, No 4/2021, 12 February 2021

Centre for Information Policy Leadership, A Path Forward forInternational Data Transfersunder the GDPR after the CJEU Schrems II Decision, 24 September 2020

Cerulus L., Cyber insights, Politico Pro, 1 February 2021

Chander A., 'Is Data Localization a Solution for Schrems II?', *Journal of International Economic Law*, Vol. 23(3), 5 September 2020

Chivot E. and Castro D., The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy, Center for Data Innovation, 13 May 2019

Christakis T. and Propp K., The legal nature of the UK-US Cloud Agreement, Cross-Border Data Forum, 20 April 2020

Christakis T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers Part 1, Part 2, Part 3, European Law Blog, 13-17 November 2020

Christakis T., 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts), European Law Blog, 17 October 2019

CJEU Judge von Danwitz T., European Data Protection Day 2021, 28 January 2020

Commissioner for Justice Didier Reynders, Presentation of two draft implementing decisions by the Commission pursuant to Regulation (EU)2016/679 and Directive (EU)2016/680 on the adequate protection of personal data by the United Kingdom, Committee on Civil Liberties, Justice and Home Affairs, 16 March 2021

Department for Business, Energy and Industrial Strategy, Written evidence PBS0024, UK Parliament, June 2020

Dickson A., Dowden: UK will diverge from 'protectionist' EU on data, Politico Pro, 11 March 2011

Duhs E., EU-UK data flows, adequacy and regulatory changes from 1st January 2021, LinkedIn, 28 December 2020

Duisberg A., 'Zertifizierung und der Mittelstand – Quo Vadis?', Zeitschrift für Datenschutz, Vol. 9(2), 2018

Frydlinger D. et al., A New Approach to Contracts, *Harvard Business Review*, September-October 2019.

Gühr A., Karper I. and Maseberg S., 'Der lange Weg zur Akkreditierung nach Art. 42 DSGVO', Datenschutz und Datensicherheit, Vol. 44(10), 2020

Hosenball M., British spy agencies see foreign ties intact despite Brexit, Reuters, 12 August 2019

Hornung G. on 'Artikel 42 DSGVO', in Eßer M. et al., *Auernhammer DSGVO BDSG*, 2020

Irion K., Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law, European Law Blog, 24 July 2020

Kelber U., Aspects where Germany's draft Federal Intelligence Services Act misses the mark, about:intel, 16 February 2021

Kim S. and Perlin P., Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance, Lawfare, 25 March 2019

Kon G. and Cumbley R., EU: Data flows post-Brexit - Choppy waters ahead?, Linklaters, 2 November 2020

Korff D. and Brown I., The inadequacy of UK data protection law: Executive Summary; Part 1: General inadequacy; Part 2: UK surveillance, Data protection and digital competition blog, 9 October-30 November 2020

Korff D., European & International Law on Trans-National Surveillance, European Parliament, 23 August 2013

Korff D., The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Data protection and digital competition blog, 3 March 2021

Korff D., Wagner B., Powels J., Avila R. and Buermeyer U., Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, University of Cambridge Faculty of Law Research Paper No 16/2017, March 2017

Lachenmann M., Data transfers between the EU and Japan: an introduction to the EU's adequacy decision on Japan, LinkedIn, 2 July 2019

Lange L.-M. and Filip A., 'Artikel 46 DS-GVO', in Wolff H. A. and Brink S., *BeckOK Datenschutzrecht*, C.H.Beck, 1 November 2020

Lowe S. and Mortera-Martinez C., Post-Brexit data transfers are not a done deal, Centre for European Reform, 29 March 2021

Maier N., Pawlowska I., Lins S. and Sunyaev A., 'Die Zertifizierung nach der DS-GVO', in *Zeitschrift für Datenschutz*, Vol. 10(9), 2020

Manancourt V., Cyber Insights: Is encryption the answer to Schrems II?, Politico Pro, 8 September 2020

Massé E., Access Now's memo on the data transfers and PNR provisions under the EU-UK Trade Agreement, accessnow, 15 January 2021

Massé E., Two years under the EU GDPR: an implementation progress report, accessnow, May 2020

McCann D., Patel O. and Ruiz J., The cost of data inadequacy, New Economics Foundation, 23 November 2020

Mildebrath H, The CJEU judgment in the Schrems II case, At a glance, EPRS, European Parliament, September 2020

Monteleone S. and Puccio L., The CJEU's Schrems ruling on Safe Harbour Decision, At a glance, EPRS, European Parliament, October 2015

Olejnik L., Technology impact of Privacy Shield invalidation - is it the EU data localization?, Security, Privacy & Tech Inquiries blog, 28 July 2020

Open Rights Group and The3million seek to appeal immigration exemption judgment, press release, Open Rights Group, 3 October 2019

Paal B. and Kumkar L., 'Artikel 42 DS-GVO', in Paal B. and Pauly D., *DS-GVO BDSG*, C.H.Beck, 2021

Patel O. and Lea N., EU-UK Data Flows, Brexit and No Deal: Adequacy or Disarray?, UCL European Institute, August 2019

Patel O. and Lea N., EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, UCL European Institute, May 2020

Patel O., Written evidence (PBS0029), UK Parliament, June 2020

Pauly D., 'Artikel 49 DS-GVO', in Paal B. and Pauly D., *DS-GVO BDSG*, C.H.Beck, 2021

Pounder C., An adequacy determination does not resolve the lower standard of data protection in the UK, Hawktalk blog, 19 November 2020

Pounder C., Draft Brexit Data Protection Regulations would undermine adequacy determination for the UK, Hawktalk blog, 18 January 2019

Propp K., Putting privacy limits on national security mass surveillance: The European Court of Justice intervenes, Atlantic Council, 21 February 2020

Rice M., What is at stake with the immigration exemption legal challenge?, Open Rights Group blog, 3 August 2018

Roßnagel A., 'Artikel 40 DSGVO', in Simitis S. et al., *Datenschutzrecht*, Nomos, 2019

Ruiz J. et al., Collect it all: GCHQ and mass surveillance, Report, Open Rights Group, 3 November 2015

Ruiz J., What the UK-Japan trade deal means for digital rights, Briefing, Open Rights Group, 5 November 2020

Schneier B., Data Mining for Terrorists, Schneier on Security blog, 9 March 2006

Sajfert J., Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy, European Law Blog, 26 October 2020

Schlender K., 'Artikel 46 DS-GVO', in Gierschmann S. et al., *Kommentar DS-GVO*, Bundesanzeiger Verlag, 2017

Schröder C., 'Artikel 47 DS-GVO' and 'Artikel 49 DS-GVO', in Kühling J. and Buchner B., *DS-GVO BDSG Kommentar*, C.H.Beck, 2018

Scott M. and Manancout V., What you need to know about EU, US and UK data talks, Politico, 2 November 2020

Selby J., Data localisation laws: trade barriers or legitimate responses to cybersecurity risks, or both?, *International Journal of Law and Information Technology*, Vol 25(3), 13 July 2017

Smith G., EU law meets state communications surveillance – what consequences for UK data protection adequacy?, Bird&Bird's DIgitalBusiness.Law, 30 November 2020

Smith G., Hard questions about soft limits, Cyberleagle blog, 15 October 2020

Smith G., What will be in Investigatory Powers Act Version 1.2?, Cyberleagle blog, 30 October 2018

Swire P., 'Schrems II' backs the European legal regime into a corner — How can it get out?, IAPP Privacy Perspectives, 16 July 2020

Taylor R., '"Data localization": The internet in the balance', *Telecommunications Policy*, Vol. 44(8), September 2020

techUK, Written evidence (PBS0050), UK Parliament, July 2020

The Commission's obligation to refuse an "adequacy decision" to the United Kingdom due to inadequacy of enforcement of personal data protection in that jurisdiction, Irish Council of Civil Liberties, 12 October 2020

The UK's Immigration Exemption in the Data Protection Act 2018 and data adequacy, Submission to the European Commission, Open Rights Group, 2 March 2021

Tielemans J., BCRs after 'Schrems II' decision: A first analysis, The Privacy Advisor, IAPP, 27 October 2020

van Eijk R. and Zanfir-Fortuna G., Schrems II: Article 49 GDPR derogations may not be so narrow and restrictive after all?, Future of Privacy Forum Blog, 4 February 2021

Warrell H., UK spy agency to use AI against cyber attacks and state actors, *Financial Times*, 24 February 2021

Werry N. and Werry S., 'Internationaler Transfer personenbezogener Daten', in Specht-Riemenschneider L. et al., *Datenrecht in der Digitalisierung*, Erich Schmidt Verlag, 2020

Witt C., Ingenrieth F. and Wittmann J., Could codes of conduct be the answer to 'Schrems II'?, The Privacy Advisor, IAPP, 29 September 2020

Wittmann J., Webinar: Implementing Codes of Conduct - Sharing Practical Experiences in Co-Regulation for Third Country Transfers post Schrems II, EU Cloud CoC, 24 February 2021

Woods L., Data Protection, the UK and the EU: the draft adequacy decisions, EU Law Analysis, 24 February 2021

Yakovleva S. and Irion K., Pitching trade against privacy: reconciling EU governance of personal data flows with external trade, *International Data Privacy Law*, Vol. 10(3), August 2020

EU-UK data flows – the lifelines of our shared digital trade – have come under pressure following the UK's withdrawal from the EU. To take regulatory and business decisions, a clear understanding of the state of play and future prospects for EU-UK transfers of personal data is indispensable. This EPRS in-depth analysis reviews and assesses trade dealings, adequacy challenges and transfer instruments under the EU's General Data Protection Regulation (GDPR).

QA-02-21-488-EN-N

This is a publication of the Members' Research Service
EPRS | European Parliamentary Research Service

PE 690.536
ISBN 978-92-846-7982-9
doi:10.2861/595569
QA-02-21-488-EN-N