# The GDPR International Data Transfer Regime: the case for Proportionality and a Risk-Based Approach

DLA PIPER

CLIFFORD
CHANCE

# Contents



# The GDPR International Data Transfer Regime: the case for Proportionality and a Risk-Based Approach

*This paper has been jointly authored by members of the Clifford Chance and DLA Piper European data protection law practice groups.*

## *Synopsis:*

*Recent enforcement action by European data protection supervisory authorities has adopted an absolutist interpretation of the European Union (EU) General Data Protection Regulation (GDPR) in the context of data transfers under Article 46 GDPR. Member State supervisory authorities have argued that it is not possible to adopt a risk-based approach when assessing transfers of personal data to "third countries", in essence arguing that transfers are prohibited if the possibility of foreign governmental access gives rise to any risk of harm (however trivial and however unlikely). In this paper we argue that such an absolutist interpretation fails to take account of both the risk-based approach on which GDPR has been built, and the principle of proportionality, a fundamental principle of both EU law and human rights law. An absolutist interpretation imposes a disproportionate burden on data exporters, violating their freedom to conduct a business enshrined in the European Charter of Fundamental Rights[1] and breaching the proportionality principle enshrined in the Treaty on European Union. It ignores the difference between the protection of a fundamental right (i.e. the rights based approach) from the calibration of the means of their protection (i.e. the risk based approach). An absolutist interpretation forces data exporters to apply the same approach and level of resources to all transfers, irrespective of the actual risk of harm to data subjects (indeed, even if there is no risk of harm whatsoever). Further, the GDPR itself and the Court of Justice of the European Union (CJEU) explicitly recognise proportionality, particularly in Article 46 of the GDPR and in various judgments of the CJEU, including the Schrems II judgment itself[2]. International data transfers are and will continue as they now form the fabric of our hyperconnected, international economy and society. An absolutist interpretation of transfer rules, which effectively amounts to a ban on most international transfers from the European Economic Area (EEA), will lead to a culture of widespread non-compliance, undermining respect for the rule of law. In this paper we argue that a risk-based, proportionate approach was the intention of legislators and the CJEU and delivers the best outcome for data subjects, exporters and wider society, by avoiding these challenges.*

1 Article 16 of the Charter of Fundamental Rights of the European Union;

2 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (C-311/18), https://curia.europa.eu/juris/liste.jsf?num=C-311/18. Commonly referred to as "***Schrems II***";

# 1. Introduction

1.1. The legal standard to be applied to personal data transfers abroad from the European Economic Area (the EEA) has been the subject of recent regulatory and judicial attention. Yet significant legal uncertainty remains, posing challenges for data exporters across the EEA and globally. This adds to compliance costs and indirectly to the charges paid by consumers for, amongst other things, information society services which rely on international data transfers. This uncertainty and the absolutist interpretation adopted by supervisory authorities in early enforcement decisions risks limiting innovation and economic development and disadvantaging organisations and ultimately data subjects within the EEA. An absolutist interpretation of transfer restrictions risks creating a blanket barrier to global data sharing with serious adverse societal impact; for example, the ability to quickly share vaccine data globally was essential to develop effective vaccines during the COVID-19 pandemic which undoubtedly saved many lives. Furthermore, this uncertainty comes at a time of acute crisis in Europe, where individuals are suffering from volatility and threats from war in Ukraine, to the energy crisis, to high rates of inflation and a painful cost-of-living crisis. This is not the time for the distraction of unnecessary and costly legal uncertainty.

1.2. There is a clear public interest in transfers continuing from Europe to "third countries" such as the U.S.[3] to support commerce and wider societal purposes[4]. There is a risk that an absolutist interpretation of transfer restrictions will create a culture of widespread non-compliance, undermining confidence in the rule of law.

1.3. An absolutist interpretation risks creating a *de-facto* ban on international transfers pursuant to Article 46 GDPR without any viable alternatives. EDPB guidance has consistently interpreted the derogations to transfer restrictions in Article 49 GDPR narrowly[5] and even where organisations have attempted to ringfence data within the EU to avoid transfer rules engaging, recent decisions by EU supervisory authorities and courts have been clear that merely localising and ring-fencing personal data in Europe may not be sufficient where the organisation processing the personal data within the EU is a subsidiary of a company subject to extra-territorial laws that may result in access to personal data by public authorities in third countries[6].

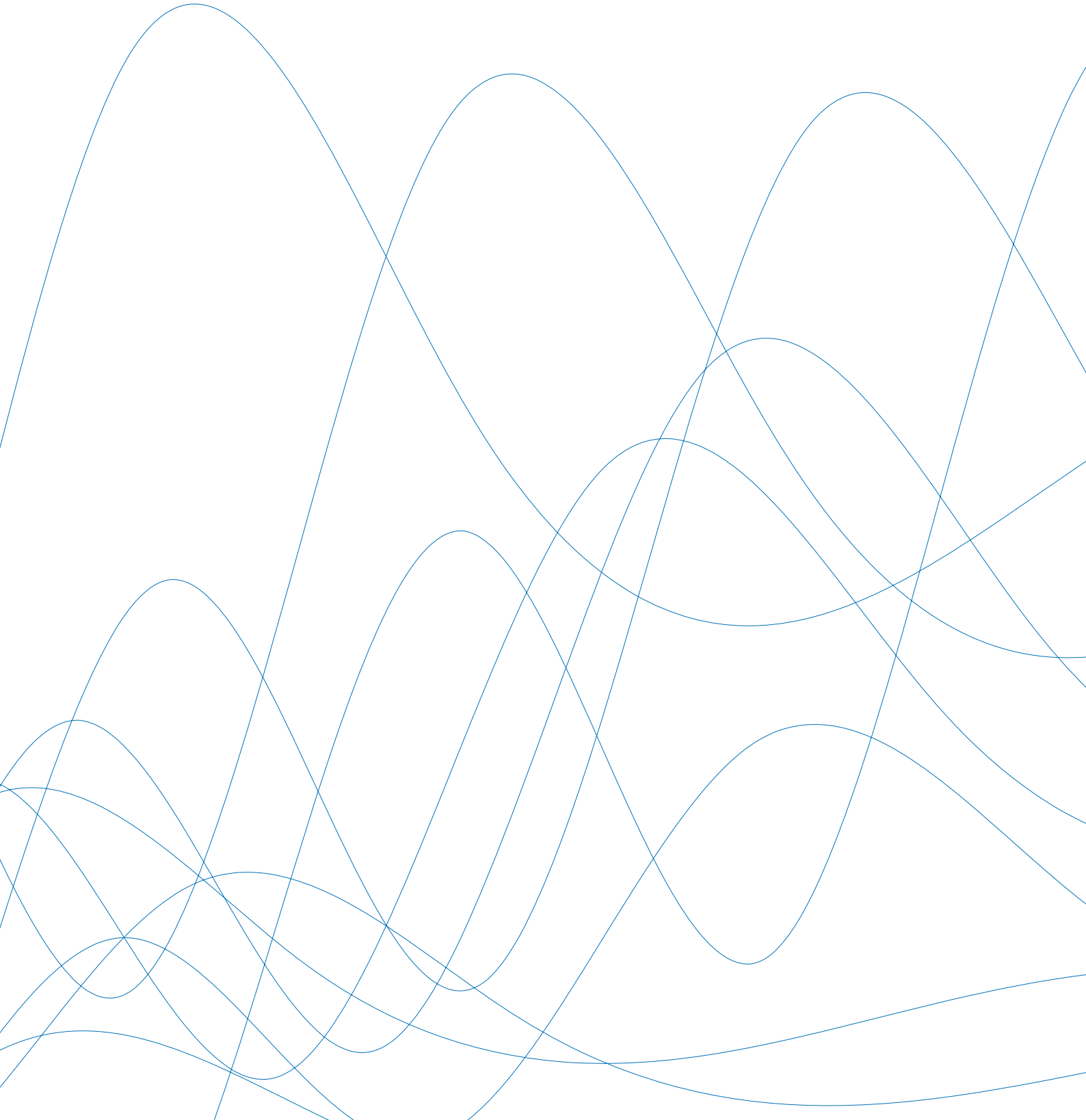
3 The authors of this paper welcome the announcement of the new EU-US Data Privacy Framework and a new US Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities" which pave the way for a new adequacy decision by the European Commission for transfers from the EU to the US. However this new US regime will only offer a partial solution and is likely to be challenged by the privacy activist Maximillian Schrems who has commented "*[a]t first sight it seems that the core issues were not solved [by the Executive Order] and it will be back to the CJEU sooner or later*." In any case, the Executive Order and any resulting adequacy decision will only address transfers to the US from the EU. The principles established by *Schrems II* and Article 46 of the GDPR apply to *all* international transfers to third countries (not just to transfers to the US);

4 There is a derogation in Article 49(1)(d) GDPR that permits transfers to third countries where "*necessary for important reasons of public interest*". However, the EDPB has stated that these derogations should be interpreted narrowly so that the exception does not become the rule. As such the derogation does not present a satisfactory alternative to transfer mechanisms under Article 46 GDPR;

5 *Ibid*;

6 For example, in March 2021 France's highest administrative court considered the application of the Schrems II decision to data hosted with an EU-based processor which was a subsidiary of a US company. The Conseil d'Etat concluded that even where there was no transfer of personal data to a third country where the EU-based service provider is a subsidiary of a company subject to US law, there was a risk that personal data could be accessed by US public authorities using extra-territorial US laws. The Conseil d'Etat press release and full decision (in French) are available here: https://www.conseil-etat.fr/actualites/actualites/le-juge-des-referes-ne-suspend-pas-le-partenariat-entre-le-ministere-de-la-sante-et-doctolib-pour-la-gestion-des-rendez-vous-de-vaccination-contre; and here: https://www.conseil-etat.fr/Media/actualites/documents/2021/03-mars/450163.pdf;

1.4. In this paper, we respectfully argue that the GDPR and relevant CJEU case law *require* a proportionate, risk-based approach be applied to personal data transfers to third countries outside the EEA. We argue that this approach is *required* to avoid a disproportionate and unlawful compliance burden and an unlawful limitation of the freedom to conduct a business; and that it is consistent with the express language of the GDPR and CJEU jurisprudence, including the *Schrems II* judgment itself.



# 2. Setting the scene: regulation of data transfers

2.1. Under the GDPR, transfers of personal data from within the EEA to third countries are subject to certain requirements, specifically under Chapter V, Articles 44 to 50. Article 44 sets the general rule that such transfers are permitted "*only if…subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor*". Article 45 provides for adequacy decisions, made by the European Commission, to allow data transfers to be made to data importers in jurisdictions recognised to provide an adequate level of protection (e.g. Switzerland). Article 46 provides that, in the absence of an adequacy decision, "*a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*". In the absence of an adequacy decision under Article 45 or appropriate safeguards under Article 46, additional derogations under Article 49 may be relied upon in specific and limited circumstances. In this paper we are principally concerned with Article 46.

2.2. Two of the (then) most prevalent mechanisms used to legitimise data transfers in accordance with Article 46 Chapter V GDPR were called into question in June 2020 in a decision of Europe's highest court, the CJEU[7]. In that case, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (C-311/18), commonly referred to as "*Schrems II*", personal data had been transferred from the EU to the US, where, it was argued, the level of protection afforded for personal data pursuant to the Privacy Shield regime was not essentially equivalent to the EU regime and, therefore, was not adequate. The CJEU agreed. It invalidated the Privacy Shield regime (a measure to ensure an adequate level of protection under Article 45 GDPR) but went further also calling into question the specific transfers under consideration in that case which relied on the then current version of the Standard Contractual Clauses (the SCCs),[8] approved by the European Commission as an appropriate safeguard under Article 46(2) GDPR. Although the Court did not invalidate the SCCs in their entirety, it held that data exporters must "verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses [such as the SCCs], by providing, where necessary, additional safeguards to those offered by those clauses"[9].

7 The specific regime in question was Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield;

8 New Standard Contractual Clauses were adopted by the European Commission on 4 July 2021 that to some extent take into account the *Schrems II* judgment. However, the new SCCs still require a risk assessment to be completed and remain susceptible to the problems created by an absolutist interpretation. See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN;

9 *Ibid*, paragraph 134;

2.3. In August 2020, multiple complaints were filed by a group associated with the privacy activist Maximillian Schrems (www.noyb.eu) against a wide range of data exporters across Europe for their continued transfer of personal data to Facebook and Google in the US in reliance on Article 46 and the SCCs, allegedly in breach of Chapter V GDPR[10]. Several of the complaints have now been addressed in decisions published by Member State supervisory authorities, notably by the Austrian,[11] French, Italian and Danish authorities[12].

2.4. The authorities specifically considered the issue of whether the GDPR allows for a risk-based approach to international data transfers made under Article 46 GDPR, by allowing a data exporter to balance the risk to the rights and freedoms of the affected individuals associated with any inconsistencies between foreign governmental access regimes and European data protection principles against the likelihood and severity of those risks and the nature and purpose of the transfer[13]. The decisions all involved the transfer of relatively low-risk data, including IP addresses, other user identifiers, and browser parameters used to provide Google Analytics.

2.5. In the published decisions, the authorities responded in the negative, i.e., that the GDPR's data transfer requirements are not subject to a risk-based approach or considerations of proportionality. They argued that, since Chapter V GDPR does not specifically refer to proportionality or risk assessment, the principles do not apply to it; and that other references to a risk-based approach and proportionality in the GDPR, such as in Article 24 (in relation to measures to ensure and demonstrate compliance with the GDPR – see further discussion below), are not applicable to Chapter V. The supervisory authorities therefore concluded that various transfers made on the basis of the SCCs were unlawful and that a risk-based approach was not permitted when applying Article 46 GDPR.

10 Details of the 101 complaints are available at www.noyb.eu;

11 See: Austrian (DSB) decisions available at: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf and https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf. French (CNIL) decision available at: https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf. Italian (Garante) decision available at: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english (document: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782890). Danish decision available at: https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics;

12 See also the decision by the Danish regulator, the Datatilsynet, which suspended the use of Google Workspace by schools, stating that the relevant Municipality had not assessed specific risks in connection with the transfer of personal data to third countries. The Datatilsynet has now temporarily lifted the ban on use of Google Workspace but stated that the permanent use of Google Workspace is conditional on the Municipality's compliance with the Datatilsynet's orders in the time period specified, these include: "a clarification of the places where the "data processor" acts as an independent data controller, as well as for what purposes, the support situations that the municipality no longer uses". See www.datatilsynet.dk/english;

13 See, for example, the French regulator's "Q&A on the CNIL's formal notices concerning the use of Google Analytics", in which the CNIL specifically states that controllers cannot adopt a risk-based approach, taking into account the likelihood of data access requests.
See: https://www.cnil.fr/en/qa-cnils-formal-notices-concerning-use-google-analytics;

2.6. These decisions are limited to their facts and are not necessarily representative of the approach taken by all EU supervisory authorities – decisions to *permit* transfers which find no infringement of the GDPR are by their nature very unlikely to be published. In each of these cases, the complaint related to transfers of personal data from Google Analytics to the United States based on the *legacy* SCCs, which in June 2021 were updated by the European Commission[14]. The new SCCs specifically require the parties to take into account "*the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the* ***specific circumstances of the transfer****, and the applicable limitations and safeguards*" (emphasis added). In addition, also in June 2021, the European Data Protection Board (the EDPB) finalised its recommendations on how organisations should comply with the *Schrems II* judgment[15]. Although not entirely clear on proportionality, the EDPB recommendations do state that data exporters can take into account "*documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country*" when carrying out a transfer impact assessment which, following the *Schrems II* ruling must now be undertaken for each transfer of personal data from within the EEA to a third country.

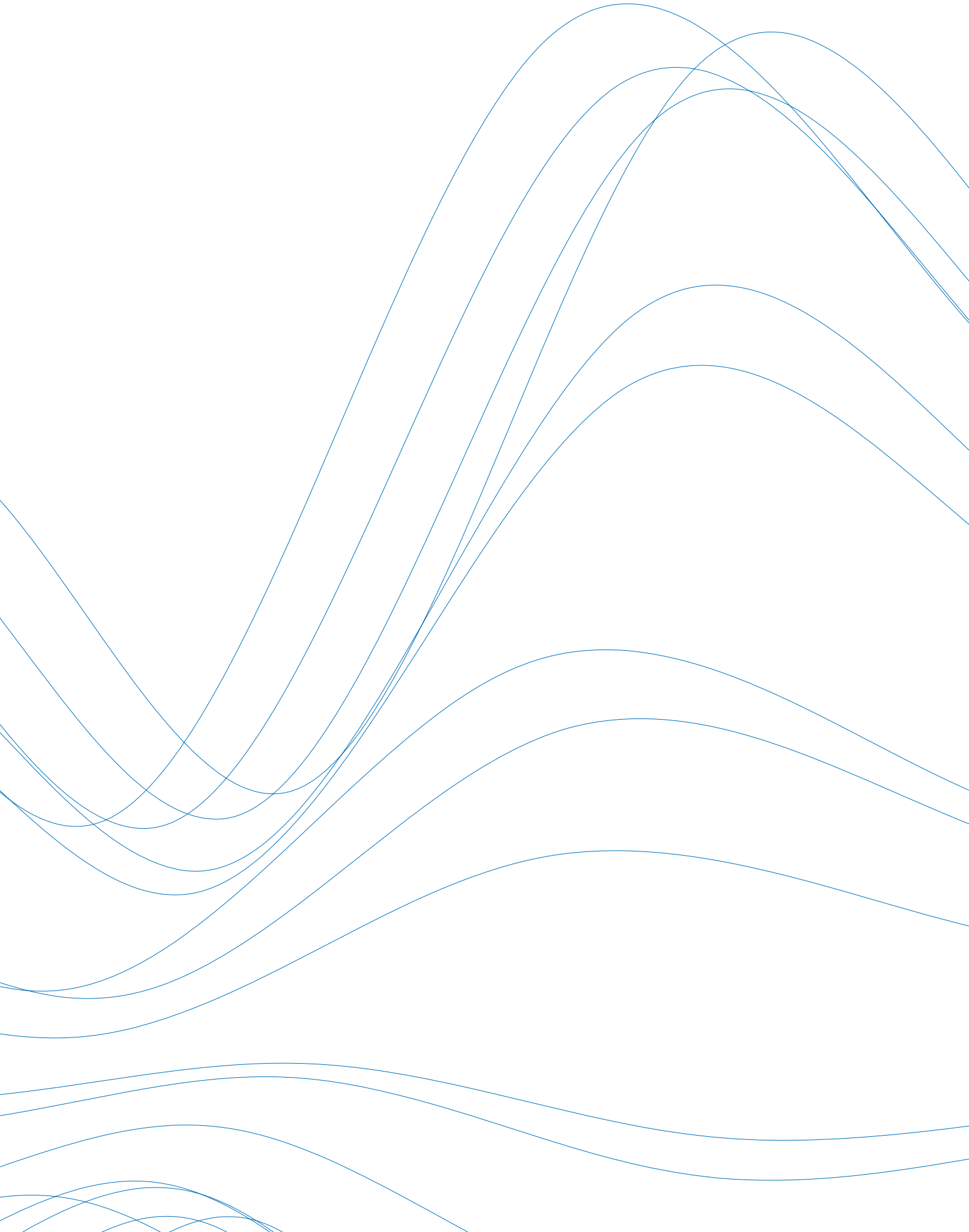
2.7. These adverse decisions do have the potential to be influential, however, and it is important in our view to explore possible alternative interpretations, in particular, that the principle of proportionality and acceptable risk make it entirely lawful and possible to transfer personal data outside of the EEA.

2.8. All the decisions to date have involved Google and are therefore heavily influenced by specific fact patterns applicable to large technology providers (specifically to Google Analytics related transfers). If followed, however, the decisions will have an adverse impact on all industries, not just technology, and pose a particular challenge for small and medium-sized enterprises (SMEs) which make up the large majority of data exporters across the *EEA*[16]. The authors of this paper acknowledge that applying the proportionality principle to risk assessments for international data transfers will mean that some higher risk transfers may not be reconcilable with the requirements of the Charter, Article 46 GDPR and *Schrems II*. We also acknowledge that there are particular risks when transferring to large technology vendors which might (though might not) exacerbate risks to the rights and freedoms of data subjects for particular transfers, but the direction of enforcement risks is setting an absolutist approach for *all* transfers as a result of concerns unique to transfers to large technology vendors. There is no need to fall into the trap of developing enforcement practice by very specific example and to dismiss proportionality and a risk based approach in their entirety – and indeed doing so is contrary to the TEU, GDPR and CJEU jurisprudence.

14 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en;

15 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en;

16 SMEs represent 99% of all businesses in the EU See: https://single-market-economy.ec.europa.eu/smes_en;



# 3. The case for proportionality and a risk-based approach

## A. Proportionality is a general and fundamental principle of EU law

3.1. All EU laws must comply with, and should be interpreted in a manner consistent with, the principle of proportionality. The principle of proportionality is a cornerstone principle of EU law, recorded in Article 5(4) of the Treaty on European Union (the TEU) as follows: "*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties*"[17].

3.2. The fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights (the Charter)[18] require appropriate protection under EU and Member State law. The protection of personal data is a fundamental right, enshrined in Article 8 of the Charter (and referred to as such in GDPR Article 1). It is one of several rights and freedoms, however, including the complementary right to respect for private and family life (Article 7 Charter) but also the freedom to conduct a business (Article 16 Charter).

3.3. The Charter provides for accepted limitations to rights, insofar as such limitations are "*provided for by law and [where the limitations] respect … the essence of those rights and freedoms.* ***Subject to the principle of proportionality****, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*" (emphasis added) (Article 51(2) Charter)[19].

3.4. In making and interpreting EU law, therefore, a balance must be struck between the means used and the intended aim, and the implications of any requirement for the freedom to conduct a business (or any other Charter right or freedom) should also be weighed in the balance. Case law provides for restrictions to rights where such restrictions "*do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights*"[20]. This limitation applies to the protection of personal data (Article 8 Charter) as well as to other fundamental rights and freedoms[21].

17 Treaty on European Union 2008/C 115/1, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2008:115:TOC. See also, Weber and Saravia v Germany, European Court of Human Rights, 29 June 2006;

18 Charter of Fundamental Rights of the European Union 2012/C 326/02. Available at: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en;

19 The Charter does not explicitly identify rights that are absolute or relative. Based on the Charter explanations, the ECHR and the case law of the European courts, certain rights including human dignity (Article 1 of the Charter), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4 of the Charter), the prohibition of slavery and forced labour (Article 5(1) and (2) of the Charter), internal freedom of thought, conscience and religion (Article 10(1) of the Charter), the presumption of innocence and right of defence (Article 48 of the Charter), the principle of legality (Article 49(1) of the Charter), and the right not to be tried or punished twice in criminal proceedings for the same criminal offence (Article 50 of the Charter) can be considered absolute rights. However, in relation to the right to protection of personal data (Article 8) the CJEU has specifically held that this right is not absolute and must be considered in relation to its function in society;

20 Case C-292/97, Karlsson and Others, Judgment of 13 Apr. 2000, para 45; Case C-11/70, Internationale Handelsgesellschaft, ECLI:EU:C:1970:114. See "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" for further detail: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf;

21 See EDPS site: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en#:~:text=Proportionality%20is%20a%20general%20principle,used%20and%20the%20intended%20aim;

3.5. It is a settled position in EU law, therefore, that the protection of personal data is a relative right, not an absolute one. The right should be implemented (and its implementation interpreted) proportionately and balanced against competing rights and freedoms, taking into account the risks involved in each data processing activity. These competing rights include the freedom to conduct a business. Accordingly, the burden and cost on data exporters of compliance with the GDPR must be taken into account as part of the risk-based approach mandated under the GDPR. An approach which excludes the application of the proportionality principle to risk assessments for data transfers, will result in an effective ban on most data transfers, exceeding what is necessary to ensure protection of personal data in the context of that right being a relative right which must be balanced against other rights and freedoms, including the freedom to conduct a business. Removing the application of the proportionality principle will also result in transfers of personal data presenting either no or low risk of harm to data subjects, such as the transfer solely of a data subject's name, requiring the same resources to assess as transfers of much richer and riskier data sets such as those comprising health data. With finite resources this will inevitably mean that exporters will be unable to prioritise and focus on protecting genuinely higher risk transfers. In short, a transfer should not be prohibited because of a problematic feature of a third country governmental access regime where the impact of the prohibition would be disproportionate to the risks of harm to data subjects associated with the transfer and in a manner which would unlawfully (i.e. disproportionately) limit other Charter rights such as the freedom for data exporters to conduct a business.

3.6. A risk-based approach enables data exporters to assess the risk associated with data transfers and apply budgets and resources to those transfers which pose a genuine risk of harm to the data subjects whose personal data are to be transferred. Legislators are well aware of the finite legal and compliance budgets and resources of data exporters, which would ordinarily be focussed on the data processing activities that do pose a genuine threat of harm to data subjects. An interpretation of the law which requires *all* personal data to benefit from the same level of protection, and require the same investment of resources, *irrespective of the risk of harm to data subjects* risks perverse outcomes, widespread non-compliance and in-effective regulation. An absolutist approach inevitably encourages 'tick-box' compliance, as data exporters will be required to carry out highly complex and burdensome transfer impact assessments of potentially multiple third country laws and practices even for the most anodyne of data sets, where there is either no or only a nominal risk of harm to the data subject. In these cases, a risk-based approach will allow exporters to avoid disproportionate compliance costs, reducing their cost base and helping to keep the price of consumer goods and services lower whilst at the same time protecting data subjects from likely as opposed to theoretical risk of harm[22].

22 See Case C-112/00, Schmidberger, [2003] ECR I-5659. In this case the ECJ recognised that "*fundamental principles… may, in certain circumstances, be subject to …overriding requirements relating to the public interest, in accordance with the Court's consistent case-law*";

3.7. All processing of personal data involves *some* risk to the rights and freedoms of data subjects. The mere existence of risk does not prohibit processing. Rather the GDPR anticipates that more protection is required if the risk of harm is higher. In the context of Article 46 GDPR and SCCs, this means that for higher risk transfers more supplementary measures would be required to mitigate those risks. But it is entirely contrary to GDPR, the TEU and the Charter to conclude that a risk-based approach to assessing transfers is not permitted simply because a transfer (like any processing) involves *some* risk to the rights and freedoms of data subjects.

## B. Proportionality applies to and is recognised in the GDPR

3.8. As to the principle of proportionality in the GDPR itself, this is expressly recognised in Recital 4, reflecting the settled law. Recital 4 provides that "*the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*". Recital 4 goes on to note that the GDPR recognises "*the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information,* ***freedom to conduct a business****, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*" (emphasis added).

3.9. The proportionality principle is settled jurisprudence of the CJEU in the context of data protection rights. In the landmark 2003 *Lindqvist* judgment of the CJEU,[23] from which many decisions and guidance have followed, the Court ruled that "*it is for the [supervisory] authorities of the Member States not only to interpret their national law in a manner consistent with Directive 95/46/EC but also* ***to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the general principles of Community law, such as inter alia the principle of proportionality. …That is a fortiori since the scope of Directive 95/46/EC is very wide and the obligations of those who process personal data are many and significant****. It is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed*."
The principle of proportionality is expressly recognised in the *Schrems II* judgment itself, where the CJEU stated that "*the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society*"[24].
An absolutist interpretation of Chapter V is therefore at odds with settled jurisprudence of the CJEU[25] and the *Schrems II* judgment itself.

23 Judgment of 6 November 2003, case C-101/01, at paragraph 87-89:

24 Paragraph 172, referring to Volker und Markus Schecke and Eifert, C-92/09 and C-93/09 and earlier case law. See also paragraph 174, referring to Article 52 of the Charter;

25 There are other examples of CJEU jurisprudence supporting the proportionality principle and a risk based approach. For example, in Breyer (CJEU – C-582/14), the CJEU explicitly invoked the principle to determine whether certain data qualified as personal data: "*…that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it required a disproportionate effort in terms of time, cost and man-power so the risk of identification appears in reality to be insignificant.*"

3.10. The application of the proportionality principle to data transfers under the GDPR is also clearly supported by a purposive interpretation of the substantive provisions of the GDPR[26]. Indeed, proportionality plays a key role in determining whether a measure is appropriate under the GDPR. This approach is enshrined in the GDPR's risk-based framework, under which controllers are required to engage in risk analysis and to adopt risk-measured responses[27]. For example, under Article 32 GDPR, controllers are required to "*ensure a level of data security appropriate to the risk*" and implement risk-based measures for ensuring compliance with the GDPR's "*general obligations*". Article 24(1), similarly, requires the controller to assess the "*likelihood and severity for the rights and freedoms of natural persons*", considering the "*nature, scope, circumstances and purposes of the processing*",[28] so at to "*implement appropriate technical and organisational measures*" such that "*the processing is performed in accordance with this Regulation [the GDPR]*". It requires the implementation of *appropriate* measures, not measures absolutely guaranteed to ensure compliance. Article 24 refers generally to the entirety of the GDPR ("*this Regulation*"); it does not exclude Chapter V and the restrictions relating to international transfers from its scope.

3.11. The GDPR's recitals note that controllers should assess the likelihood and severity of the risk to the rights and freedoms of the data subject, which should be determined "*by reference to the nature, scope, context and purposes of the processing examples of harms and require controllers to assess the* ***probability of such harms****, considering the nature of the threat*" (emphasis added)[29]. The GDPR also imposes heightened requirements on controllers that engage in 'high-risk' activities, in particular Article 35 GDPR states that "*where a type of processing (…) is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact (…) on the protection of personal data*." A risk-based approach is also apparent in Article 33 of the GDPR, which states that a data breach must be notified to the supervisory authority, "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*". Furthermore, the EDPB and the European Commission have also indicated that a risk-based approach should be applied to data transfers, requiring data exporters to adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence, depending on "*the context of the transfer, and in light of the third country law and practices*". Thus, an absolutist interpretation would be inconsistent with both the language and the scheme of the GDPR; as well as being anathema to the requirements of the TEU and Charter and settled jurisprudence of the CJEU.

26 A purposive interpretation of the law is well established by the CJEU, which will interpret EU law to give effect to the aim or spirit of the legislation, taking into account its context and general objectives. The CJEU sums up its interpretive approach in van Gend en Loos (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61962CJ0026), stating "*it is necessary to consider the spirit, the general scheme and the wording*";

27 The purpose limitation (Article 5(1)(b) GDPR) itself embodies proportionality reasoning at a general level. Other articles of the GDPR provide for proportionality reasoning, including Articles 6(1)(f), 23, 35, 83, 84, and 90;

28 "Processing" includes transfer, under Article 4(2) GDPR, which defines processing as "any operation or set of operations which is performed on personal data", including transmission and dissemination or otherwise making available;

29 Recital 76 GDPR;

## C. Proportionality is built into Chapter V GDPR

3.12. Article 52(1) of the Charter, which includes the principle of proportionality, applies to the entirety of GDPR. No special exception is made for the restrictions on international transfer set out in Chapter V GDPR. Similarly, in GDPR itself, Article 24(1) explicitly calls for appropriate measures designed to ensure that "*processing is performed in accordance with **this Regulation***" (emphasis added – that is, the whole of the GDPR, including Chapter V) – its standard of appropriateness clearly applies to the measures implemented to comply with Article 46, which would be inconsistent with an absolutist interpretation of Article 46 itself.

3.13. Article 46, as discussed above, establishes that a transfer may take place if there are "***appropriate** safeguards, and on condition that **enforceable** data subject rights and **effective** legal remedies for data subjects are available*" (emphasis added). This is not an absolutist requirement, clearly identifying appropriateness, and for considerations of the inherently flexible concepts of effectiveness and enforceability, as factors to be considered when assessing whether the safeguards ensure a level of protection for personal data in the transferee jurisdiction that is essentially equivalent to the EEA. This assessment is based on an analysis of the risks involved in a transfer, such as "*examining the practices in force in the third country*"[30]. Even a literal reading of Article 46 therefore indicates that an assessment of the transferee jurisdiction should be based on an analysis of the risk, a reasonable and sensible application of the proportionality principle to the right to the protection of personal data of the specific transfer in scope.

3.14. Finally, the jurisprudence of the CJEU recognises that the proportionality principle is at the heart of the interpretation and application of data protection rights as discussed in paragraph 3.8 above. The *Schrems II* ruling of the CJEU itself explicitly calls for "*all the circumstances of the transfer*"[31] to be considered when determining whether Standard Contractual Clauses can be complied with by a data importer in a third country. As with Article 46, the CJEU also clearly contemplated that an assessment of the transferee jurisdiction should be based on an analysis of the risk and the application of the proportionality principle, rather than an absolutist interpretation.

30 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2, paragraph 43, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. See also *Schrems II*, para 126;

31 Paragraph 121, *ibid*.

# 4. Conclusion

4.1. The *Schrems II* judgment has created significant legal uncertainty and challenges for data exporters across the EEA requiring highly complex assessments of the laws and practices of third countries and risk assessments. The absolutist interpretation adopted by some data protection supervisory authorities in early enforcement of the principles established in *Schrems II* and Article 46 has compounded this challenge. An absolutist approach is contrary to the Charter, the Treaty on European Union and GDPR all of which apply the principle of proportionality to data protection as a relative, rather than absolute, right. GDPR also requires a risk based approach when protecting the right to data protection as explicitly set out in Article 24 GDPR. An absolutist approach is also contrary to landmark jurisprudence of the CJEU, including the *Schrems II* judgment itself. Adopting an absolutist approach will inevitably result in a culture of widespread non-compliance, undermining the rule of law and is also contrary to the law.