COURT OF JUSTICE OF THE EUROPEAN UNION

Written observations by BSA | The Software Alliance

Submitted in accordance with Article 23, second paragraph of the Statute of the Court of Justice of the European Union, by BSA | The Software Alliance, party to the national proceedings before the High Court (Ireland), represented by Bart Van Vooren and Kristof Van Quathem,[1] attorneys-at-law at Covington & Burling LLP (Kunstlaan 44, 1040 Brussels, Belgium), who declare that all communication may be submitted by means of the e-curia platform and/or by email to bvanvooren@cov.com, in the reference for a preliminary ruling from the High Court (Ireland) made in the case.

C-311/18

Data Protection Commissioner

v

Facebook Ireland Limited, Maximillian Schrems.

To the President and the Members of the Court of Justice of the European Union, BSA | The Software Alliance submits the following written observations to the Court.

[1] The attorneys refer to the notice to be added as representatives for BSA | The Software Alliance, including the Power of Attorney attached thereto, submitted to the CJEU registry on 11 September 2018 by William Fry.

I. Summary of written observations on the questions referred by the Irish High Court

1. This proceeding arises from a referral to the Court of Justice of the European Union ("CJEU" or "Court") by the Irish High Court. It centres on Commission Decision 2010/87/EU, OJ L 39, as amended (the "SCC Decision"), which provides the legal basis for transfers of personal data from the Union to third countries around the world.[2]

2. While the Irish High Court has referred eleven questions to the CJEU, this case in fact turns primarily on a single issue: whether the SCC Decision provides "adequate safeguards" as required by the Data Protection Directive for the transfers of personal data contemplated in this case.

3. BSA | The Software Alliance ("BSA") submits that the answer to this question is "yes." BSA is a multinational technology trade association that brings together the world's leading software companies.[3] These companies, and their many enterprise customers across Europe, rely on the SCC Decision to transfer personal data across the globe every day. Our members have extensive first-hand experience with the SCC Decision and can attest to the robustness of its safeguards.

---

[2] The European Commission has adopted three SCC Decisions: Commission Decision 2001/497/EC, OJ L 181, and Commission Decision 2004/915/EC, OJ L 385 ((EU-)controller to (Non-EU/EEA-)-controller clauses) and Commission Decision 2010/87/EU, OJ L 39 ((EU-)controller to (Non-EU-)processor clauses) as amended by Commission Implementing Decision (EU) 2016/2297, OJ L 344. This referral – and therefore BSA's submission – is focused on only one of the SCC Decisions: Decision 2010/87/EU. Because this Decision was adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 (the "**Data Protection Directive**"), this submission similarly references that Directive and not the legislation that has replaced it (i.e., Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "**General Data Protection Regulation**" or "**GDPR**")).

[3] BSA's members include: Adobe, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, Microsoft, McAfee, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

4. The Irish High Court, in framing its referral questions, largely ignores the SCC Decision's many safeguards, however. Instead, the Court's questions largely focus on the adequacy of the safeguards afforded to personal data *under U.S. law*.

5. In doing so, the Irish High Court fails to recognise that the strength of the safeguards provided by the SCC Decision, and the standard contractual clauses appended to the Decision ("SCCs"), are not contingent upon the adequacy of any other country's legal regime. Instead, the SCCs are specifically designed for transfers to countries whose data protection regimes have *not been deemed adequate* by the European Commission ("non-adequate" countries[4]). The adequacy of the U.S. regime – or any other third country's regime – is therefore not dispositive to the case before the Irish High Court.

6. In adopting the SCC Decision in 2010, the European Commission acted in accordance with the authorisation of the EU legislature as expressed in the Data Protection Directive. That Directive provides that a data controller may lawfully transfer personal data from the Union to a non-EU country (a "third country") only if either: (i) the third country's legal regime for the protection of personal data has been deemed "adequate" by the Commission (Article 25); *or* (ii) a country's regime has not been deemed adequate, a derogation applies (Article 26). Among the derogations set forth in Article 26 is the one at issue here – namely, the ability to transfer data pursuant to contractual provisions that ensure that "the controller adduces *adequate safeguards* with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights." (Article 26(2)).

7. Consistent with Article 26(2), the SCC Decision imposes a range of contract-based obligations on transferors and recipients of personal data. These obligations – which are legally binding and fully enforceable under Union law – ensure that the Data Protection Directive's protections flow with any data transferred under the Decision. In this way, the SCCs provide robust protections for EU data subjects even in cases in which the third country's data protection law is not equivalent to that of the Union, and even in cases in

[4] In using the term "non-adequate country" here and elsewhere in this submission, we do not suggest that the U.S. regime could not meet the necessary standards to demonstrate adequacy. Instead, we use the term simply to describe those third countries that the European Commission has not assessed for adequacy.

which that domestic law may not accord with the SCCs. For example, in recognition of the fact that third countries might not offer sufficient judicial relief to EU data subjects, the SCC Decision and the SCCs include provisions that give data subjects meaningful remedies under EU law and before EU supervisory authorities.

8. The SCCs are indispensable to the ability of European enterprises to participate in the global economy. Cross-border data transfers are essential to international commerce and communication – but the vast majority of the EU's trading partners have not been deemed adequate under Article 25. The SCCs fill this gap. Today, the SCCs underpin transfers of personal data from the Union to over 180 countries – including Australia, Singapore, South Korea, Brazil, India, Mexico, and many others. Without the SCCs, most European enterprises would be forced to significantly curtail their interactions with parties outside the EU, or alternatively to rely on other derogations in Article 26, many of which offer fewer protections than the SCCs. For example, under the Directive, if a data subject consents to a transfer to a non-adequate third country, *no* safeguards or means of redress are provided.

9. In light of the SCCs' purpose – to enable transfers to *non-adequate* countries – the central question that the Irish High Court should have considered is not whether a third country adequately protects data transferred. That is because the SCCs themselves provide these protections. Instead, the central question is whether the controller has afforded the "adequate safeguards" required by the Directive in the particular context of the transfers at issue.

10. The assessment requires the supervisory authority to conduct a case-by-case analysis of the specific transfer in issue that considers all relevant circumstances. There is no "one-size-fits-all" adequate safeguard. Instead, factors such as the type of data involved, the protections afforded by the SCCs, and any additional protections offered by the controller or processor, and the purposes of the processing are all relevant in determining whether safeguards are adequate.

11. Consistent with the above, in this submission, BSA will:
    a. describe the unique importance of the SCCs to global data flows (Section II);

b. recount the legal underpinnings of the SCC Decision and explain why the adequacy of the U.S. (or any other country's) legal regime is not dispositive of the lawfulness of transfers made under it (Section III);
c. summarise the protections afforded data subjects by the SCC Decision and SCCs, and demonstrate that these safeguards are adequate within the meaning of Article 26(2) – regardless of the law of the country of destination (Section IV); and
d. provide our observations on those questions that we believe are dispositive for the resolution of the matter before the Irish High Court – specifically, questions 6, 7, 8 and 11 (Section V).

II. The SCC Decision is indispensable to global data flows today

12. As the Court is well aware, the ability to transfer personal data across borders is an indispensable element of the global economy. Global communications and commerce simply cannot happen without transfers of personal information.

13. Because the SCC Decision enables transfers to virtually any country in the world, the SCCs have become among the most important and widely used mechanisms for cross-border transfers of personal data from one enterprise to another. Thousands of companies use the SCCs for millions of data transfers to countries all over the world every single day for routine business purposes including the sale and supply of goods and services, the recruitment, training, and management of staff, and the general administration of business – precisely as the EU legislature intended.

14. For example, EU companies frequently rely on the SCCs to enable remote IT or customer support service providers to access EU personal data; in this way, EU companies and their customers can enjoy round-the-clock services provided by operators in different time zones. EU companies with multinational operations also transfer personal data pursuant to the SCCs in order to create corporate-wide email address books, which allow EU-based employees to communicate with colleagues elsewhere. SCC-based transfers are also core to many other transfers, including those necessary to the operation of the Internet and technology innovation, to collaboration among universities and researchers around the world, and to NGOs with global operations.

15. The reliance of businesses on the SCCs was highlighted in the IAPP-EY Annual Privacy Governance Report 2016, which found that 89% of non-government EU firms transfer personal data from the Union to the United States using the SCCs, making it the most relied upon mechanism for such transfers.[5] A recent survey conducted by BSA and the U.S. Chamber of Commerce reinforces the importance of the SCCs.[6] Of those companies that responded, all use the SCCs for transfers of personal data from the Union to countries around the world; 70 percent rely on the SCCs as their principal data transfer mechanism; and half have over 1,000 SCCs in place.

16. Given the importance of the SCC Decision to global communications and commerce, its invalidation would have dramatic economic consequences for companies across Europe, in particular for small and medium-sized businesses that rely on third-party services (e.g. cloud computing, data security, and other services) to compete. Invalidation of the SCC Decision might even force European firms to cease certain business operations altogether.

17. Invalidation of the SCC Decision would also significantly diminish privacy protections for EU data subjects. As explained above, the SCCs contractually commit non-EU data importers to provide specific, enumerated protections for EU data subjects and their personal data. This is in direct contrast to other transfer mechanisms under Article 26. If the SCC Decision is struck down, European organizations in many cases would have no alternative but to rely on consent or other derogations that provide *fewer safeguards* for personal data transferred abroad than are available under the SCCs.

III. The SCC Decision is specifically designed for transfers to third countries whose legal regimes have not been deemed adequate

18. Article 25(1) of the Data Protection Directive lays down the general principle that transfers of data from the Union to third countries "may take place only if . . . the third country in question ensures an adequate level of protection." Article 25(2) in turn establishes the

[5] *See* the IAPP-EY Annual Privacy Governance Report 2016, page 98 (available at: https://iapp.org/media/pdf/resource_center/IAPP%202016%20GOVERNANCE%20SURVEY-FINAL3.pdf),

[6] *See* Annex A.1.1.

relevant criteria to assess whether the level of protection within a third country is "adequate" for purposes of Article 25(1).

19. Article 25(6) empowers the European Commission to determine that a non-EU country ensures an adequate level of data protection, within the meaning of Article 25(2), by reason of its "domestic law or of the international commitments it has entered into." When the Commission makes such a determination, it issues a Decision – often referred to as an "Adequacy Decision" – enabling organizations to transfer personal data freely to that non-EU country without any additional safeguards being in place.

20. Most countries in the world – over 180 – have not been assessed as providing an adequate level of data protection, however.[7] If the Union were to prohibit transfers of personal data to all of these countries, EU commerce with most of the world's economies would be hobbled; personal data would largely be held captive in Europe, thwarting the ability of European business to operate and transact across EU borders.

21. In recognition of this fact, EU legislators decided not to prohibit altogether the transfer of personal data to countries that have not been deemed adequate. Instead, EU legislators adopted, in Article 26 of the Directive (entitled "Derogations"), a series of exceptions to Article 25 that authorise transfers to non-adequate countries under certain conditions.

22. Article 26(2) of the Directive allows a Member State to authorise transfers to a third country "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights." The derogation explicitly provides that "such safeguards *may in particular result from appropriate contractual clauses*."

23. Article 26(4) of the Directive in turn empowers the European Commission to decide that "certain contractual clauses offer sufficient safeguards as required by [Article 26(2)]." The

[7] Only nine countries and three regions have been deemed "adequate" in the 22 years since the Data Protection Directive's adoption. This list includes Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, the United States (in relation to data transferred pursuant to the EU-U.S. Safe Harbour, and now EU-U.S. Privacy Shield), and Uruguay.

Commission has relied on this provision to publish three sets of SCC Decisions, enabling EU data controllers to transfer personal data to both processors and controllers in third countries that have not been deemed adequate.[8]

24. Article 26, and the SCC Decisions adopted under it, are therefore specifically designed to address scenarios in which data will be transferred to a non-adequate country. Accordingly, whether or not a third country's legal regime provides an "adequate level of protection" is wholly irrelevant to the analysis of whether a derogation under Article 26 is valid and may lawfully be utilised to transfer personal data to a third country. To the contrary, Article 26 is concerned with *precisely the scenario in which a third country does not provide an adequate level of data protection.*[9]

25. The legislative history of the Data Protection Directive confirms that the derogations e in Article 26 were intended to be exceptions to the principles set out in Article 25. Two years after originally proposing the Directive, and following stakeholder consultation and multiple opinions from the European Parliament, the Commission concluded that "it became clear that in certain cases there would have to be exceptions to [the prohibition on data transfers contained in Article 25]," and proposed "that the ban on transfers to non-member countries which do not provide an adequate level of protection should be subject to exceptions compatible with the protection of individuals."[10] Accordingly, the Commission introduced new, more prescriptive, language into the draft Data Protection Directive, including the following: "A Member State may authorise a transfer or category of transfers of personal data to a third country *which does not ensure an adequate level of protection* where the controller adduces sufficient justification in particular in the form of *appropriate contractual provisions* guaranteeing, especially, the effective exercise of data subjects' rights."[11] This language ultimately became the current wording for Article 26.

---

[8] *Infra.* Footnote 2.

[9] Accordingly, the adequacy finding afforded the United States by the European Commission for transfers pursuant to the EU-U.S. Privacy Shield is unrelated to the ability of controllers to avail themselves of SCCs for data transfers to the United States.

[10] *See* Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final, page 35.

[11] *Ibid.*, Article 27.

26. Guidance from Member State supervisory authorities (then the Article 29 Data Protection Working Party) reinforces the view that Article 26 is meant to enable transfers to non-adequate jurisdictions. Their guidance explains that contracts are "a means by which adequate safeguards can be provided by the data controller when transferring data outside of the Community … to a third country where the general level of protection is not adequate."[12] Of particular relevance to this case, the Article 29 Data Protection Working Party was clear that using contractual clauses can "*make up for the absence of oversight and enforcement mechanisms*"[13] in a third country not deemed to offer an adequate level of data protection.[14] This is because the SCCs themselves ensure that EU data subjects are provided "oversight" of their rights by EU authorities, and the ability to "enforce" these rights in EU courts – thus rendering questions about the adequacy of oversight and enforcement mechanisms available under the laws of the third country irrelevant.

27. Thus, in adopting Article 26, EU legislators clearly determined that contractual protections in the form of SCCs *can* provide adequate safeguards for EU personal data transferred to third countries whose laws do not provide adequate protection for such data. Were this Court to overrule that determination, it would override the express views of the Union legislature, nullify Article 26(2), and hold instead that data can flow *only* if a third country's legal regime has been deemed adequate in accordance with Article 25. In effect, for enterprises in the Union to participate in global trade, the CJEU would require that the laws of virtually every country in the world be deemed essentially equivalent to those in the Union.[15]

---

[12] *See* Article 29 Data Protection Working Party Opinion on the Protection of Individuals with regard to the Processing of Personal Data (WP 12), page 16.

[13] *Ibid*., page 18.

[14] In this regard, we note that the regulation that has replaced the Data Protection Directive – the GDPR – also allows personal data to be transferred to non-adequate third countries on the basis of "standard data protection clauses adopted by the Commission." (Article 46(2)(c)). The GDPR equally makes clear that a finding of adequacy or non-adequacy is "without prejudice to transfers of personal data to the third country [on the basis of the standard data protection clauses]." (Article 45(7)).

[15] As one contemporaneous Council document explains, legislators were particularly concerned that such an approach would give "the impression of a certain imperialistic attitude" and validate the view of some third countries that the Union was seeking to create a "European fortress." *See* Council Outcome of Proceedings of Working Party on Economic Questions (Data Protection) on 23 and 24 July 1991, 7767/91, July 31 1991, pp. 13-15. (*see* Annex B.1.1).

IV. The SCC Decision and SCCs provide "adequate safeguards" for personal data transferred under them

28. As set out in paragraph 22 above, Article 26(2) of the Data Protection Directive allows for transfers to jurisdictions not deemed adequate only if the controller "adduces adequate safeguards" to protect the privacy and fundamental rights and freedoms of the individuals whose data is transferred.

29. To ensure that controllers adduce such safeguards, the SCCs impose a wide range of obligations on data exporters (i.e. transferors of personal data) and importers (i.e. recipients of that data) to protect transferred data. These obligations materially reflect the obligations in the Data Protection Directive, which in turn are consistent with the rights enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (the "Charter").

30. Pursuant to the SCCs, for example, data exporters must ensure that processing in the third country will be carried out in compliance with the exporter's domestic data protection law (i.e. Union or Member State law), and must instruct the data importer to process transferred data only in accordance with that law and with the SCCs. In effect, the SCCs require that the Directive's data protection obligations continue to apply to personal data even after it is exported to a third country. Exporters must also warrant that the importer will provide sufficient security measures to protect the data, and must carry out an evaluation of those measures prior to transfer; must inform data subjects if sensitive data is being transferred to a non-adequate jurisdiction; and must ensure that processing by sub-processors meets similarly high standards.[16]

31. Although the safeguards in the SCC Decision and the SCCs are contractual in nature, this does not render them any less meaningful. To the contrary, the SCCs include several

[16] The extensive safeguards contained in the SCCs were adopted after an exhaustive process of consultation and consideration that sought and reflected the views of all EU institutions and the Member States. *See* Article 26(4) and Article 31(2) of Data Protection Directive. Scrutiny and negotiations around the second set of "controller to controller" SCCs (enacted by Commission Implementing Decision 2004/915/EC, OJ L 385), for example, lasted approximately eight years. *See* Kuner, C, Improper Implementation of EU Data Protection Law Regarding Use of the Standard Contractual Clauses in Germany (October 6, 2006). Available at SSRN: http://ssrn.com/abstract=1444813 (page 5).

"safety valves" specifically designed to ensure that data subjects are protected even when data is transferred to countries whose domestic law is inadequate, and even if that domestic law may not provide judicial redress for breaches of the SCCs.

32. First, the SCCs require a data importer to warrant that it will process data in compliance with the data exporter's instructions (which must, in turn, comply with the Data Protection Directive).[17] The data importer must also warrant: (i) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract; and (ii) that, if the applicable legislation changes in a way that is likely to have a substantial adverse effect on the warranties and obligations set forth in the SCCs, the importer will promptly notify the change to the data exporter, in which case the data exporter may suspend the transfer of data and/or terminate the contract.[18] This ensures that, to the extent there is a conflict between the importer's obligations under domestic law and its obligations under the SCCs (including in relation to national security obligations placed on the importer), the exporter is made aware of this conflict and can suspend data flows in response.

33. Second, the SCCs restrict an importer's authority to derogate from its obligations under the SCCs in order to comply with an obligation under domestic law. A derogation is allowed only if the domestic law imposes a "mandatory requirement" that does not "go beyond what is necessary in a democratic society . . . that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses."[19] This derogation draws directly from EU law. The condition, "necessary in a democratic society," derives from Article 8 of the European Convention on Human Rights,[20] and has been further developed in the case law of the European Court of

[17] *See* SCC Decision, Clause 5(a).

[18] *Ibid.*, Clause 5(b).

[19] *Ibid.*, Clause 5, footnote 1.

[20] Article 8(1) of the European Convention on Human Rights provides for the right to respect for private and family life, and Article 8(2) states that "There shall be no interference … with the exercise of this right except

Human Rights.[21] It is also included in Council of Europe Convention No. 108.[22] The Data Protection Directive contains a similar derogation, set out in Article 13;[23] a similar derogation is also set forth in Article 52 of the Charter.[24]

34. Third, remedies for breaches of SCC obligations are not limited to the parties to the contract (i.e. the data exporter and data importer). Instead, the SCC Decision provides *data subjects* with mechanisms to obtain redress for such breaches, including against the data exporter, the data importer, and third parties responsible for processing data on their behalf.[25] For example:

    a. *Data subject right to sue / seek court orders*. The SCCs make the data subject a third-party beneficiary of the clauses, conferring on affected data subjects the right to sue the exporter, and under certain circumstances the importer, for damages suffered as a result of breaches of the SCCs by any party or subprocessor.[26]

---

such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[21] *See Handyside v. United Kingdom*, Judgment of 7 December 1976, Series A No.24 (1979-80) 1 EHRR 737; The *Sunday Times v. UK*, Judgment of 26 April 1979, 2 EHRR 245.; *Klass v. Germany*, Judgment of 6 September 1978, Series A No.28; (1979-80) 2 EHRR 214.

[22] *See* Council of Europe Convention, No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 9(2). Article 9(2) states "[d]erogation from . . . this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; (b) protecting the data subject or the rights and freedoms of others."

[23] Article 13 of the Data Protection Directive states that "(1) Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in [specified articles of the Directive] when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences…." Similar provisions are now found in Article 23 of the GDPR.

[24] Article 52(1) of the Charter states that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and 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."

[25] As the Commission explains in the SCC Decision, "[s]tandard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract." *See* SCC Decision, recital 19.

[26] *Ibid.*, Clauses 3(1) and (2) and Clauses 6(1) and (2).

b. *Fall-back remedies*. Even in cases in which the data exporter cannot be sued (e.g. because it has ceased to exist), the data subject can still assert claims against the non-EU data importer or its non-EU sub-processors. [27]

c. *Regulatory oversight*. The parties contractually commit to cooperate with the applicable Member State supervisory authorities, which ensures that these authorities retain regulatory oversight of their activities at all times.[28]

d. *Extraterritorial reach of investigation*. Data subjects can also complain directly to a Member State supervisory authority. Further, the data exporter and data importer commit to the supervisory authority having the power to conduct audits, even of the importer, thereby consenting to the authority's jurisdiction over their actions regardless of where those actions occur.[29]

e. *Disputes resolved under local law*. Importantly, any dispute between the data subject and the data exporter is to be resolved in accordance with the governing law of the data exporter (i.e. EU law)[30] – *not* the law of the country to which the data was exported. This extraterritorial dimension of the SCCs allows data subjects to invoke Union law to delineate the parameters of, and enforce, the safeguards described above. The parties also commit to abide by the final and binding decisions of competent courts of the data exporter's country of establishment.

35. These remedial mechanisms are available to data subjects irrespective of a third country's laws and practices. In other words, regardless of whether the third country's legal regime affords EU data subjects adequate judicial redress, the SCC Decision ensures that effective redress is available, consistent with the Charter.[31]

---

[27] *Ibid.*, Clauses 3(2) and (3), and Clauses 6(2) and (3).

[28] *Ibid.*, Clause 8.

[29] *Ibid.*, Clause 8(2).

[30] *Ibid.*, Clause 9.

[31] *Ibid.*, Clauses 6 and 7. The EU legislature, in the GDPR, expressly recognises that it is sufficient to offer data subjects remedial measures in the Union to the extent that a third country's legal regime may otherwise be inadequate. Recital 108 of the GDPR provides that "In the absence of an adequacy decision, the controller . . . should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. . . . Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union *or* in a third country."

36. Finally, the SCC Decision does not restrict the ability of supervisory authorities to exercise their powers to examine claims from data subjects afforded to them under Article 28 of the Data Protection Directive, or to intervene with respect to specific transfers. Article 28 confers on supervisory authorities powers to, for example, investigate alleged breaches of the Directive or the SCCs, and to require that the responsible controller add further safeguards or cease transferring personal data.

37. As the SCC Decision explains, "a Commission decision adopted pursuant to Article 26(4) of Directive 95/46/EC is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities, in so far as it has the effect of recognising that transfers taking place on the basis of standard contractual clauses set out therein offer sufficient safeguards as required by Article 26(2) of that Directive. *This does not prevent a national supervisory authority from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses*."[32]

38. This position flows from the CJEU's judgment in *Schrems I,* in which the CJEU held that "in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with Union rules concerning the protection of individuals with regard to the processing of personal data" and that "each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46."[33]

[32] Commission Implementing Decision (EU) 2016/2297 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, OJ L 344, recital 5.

[33] *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650, paragraph 47.

V. Observations on the questions posed by the Irish High Court

39. The Irish High Court has referred eleven questions to the CJEU. The majority of these – specifically, questions 2, 3, 4, 5, 9 and 10 – relate to whether the U.S. legal regime provides an "adequate" level of protection for the data at issue.[34]

40. As explained above, the legality of the SCC Decision is entirely independent of the adequacy of the U.S. legal regime. An invalidation of the SCC Decision based on alleged deficiencies of one country's legal regime would misunderstand the role of the Article 26 derogations, and the SCCs in particular. An invalidation would also disregard the EU legislature's explicit decision to allow for the use of contractual protections as a basis for transfers of personal data to third countries. For this reason, this Court need not address questions 2, 3, 4, 5, 9 and 10.

41. Of the questions referred by the Irish High Court to the CJEU, only questions 6, 7, 8 and 11 raise issues relevant to this proceeding.

42. Question 6 asks, in effect, what "level of protection" must be afforded to data transferred from the Union to third countries pursuant to the SCCs in light of Articles 25 and 26 of the Data Protection Directive and the Charter, and what factors should be considered in assessing whether this level of protection is met.

43. As set out above, Article 26 makes clear that, in assessing the appropriate level of protection, the protections afforded by the legal regime in the country of transfer, and whether those protections meet Charter requirements or are otherwise essentially equivalent to those available in the Union, are irrelevant. The key question under Article 26 is whether the protections afforded by the SCC Decision and SCCs provide "adequate safeguards" *in light of the absence of such protections in the country of transfer.*

44. In making this assessment, the supervisory authority must determine whether, on balance, the safeguards deployed will adequately "respect . . . the protection of the privacy and

[34] BSA does not express a view on question 1. We believe that the European Commission and the Member States are best-placed to respond to that question.

fundamental rights and freedoms of individuals and . . . the exercise of the corresponding rights," as required by Article 26(2) of the Data Protection Directive. In effect, this requires the supervisory authority to assess whether the transferred data and the data subject will receive materially the same protections as afforded in the Data Protection Directive."[35]

45. The assessment of whether the safeguards applied by a controller to a particular transfer are adequate must be made on a case-by-case (i.e. transfer-by-transfer) basis. The supervisory authority must consider the totality of the circumstances involved in the transfer, including the type of personal data being transferred and the characteristics of the processing operations concerned, the safeguards provided by the specific contractual clauses at issue, and any further safeguards provided by the data exporter and / or the data importer, among other considerations. This case-by-case assessment allows supervisory authorities to weigh the specific safeguards afforded by the SCCs and other measures adopted by the controller against the risk of interference with the rights of data subjects.[36]

46. If the supervisory authority concludes that protections are insufficient for a given transfer, the authority has the power to suspend the relevant transfer or otherwise block the processing, among other remedial measures. The supervisory authority does not, however, have the ability to pass judgment on the lawfulness of the SCC Decision itself. That is left to the judgment of the CJEU, which must consider whether the SCC Decision and SCCs allow a data exporter to transfer data in compliance with EU law, taking in to account the safeguards they include, the remedies they make available to data subjects, and the power of supervisory authorities and of Member State courts to intervene where appropriate.[37]

---

[35] *Schrems I*, paragraph 47 explains that "[a]s, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46."

[36] Significantly, in the GDPR, legislators replaced the term "*adequate* safeguards" with the term "*appropriate* safeguards" – reinforcing the current position, i.e. that any assessment of safeguards must consider the totality of the circumstances surrounding the transfer and whether the safeguards imposed are appropriate to the risk. *See*, e.g. GDPR Article 46 (titled "Transfers subject to *appropriate* safeguards").

[37] *See Schrems 1*, paragraph 62 ("Whilst the national courts are admittedly entitled to consider the validity of an EU act . . . they are not, however, endowed with the power to declare such as act invalid themselves. . . .").

47. Question 7 asks whether the fact that the SCC Decision imposes a contractual remedy between the data importer and exporter, rather than a statutory remedy binding on third-country authorities, precludes the SCC Decision from adducing adequate safeguards.

48. The answer to this question is "no." The fact that the SCC Decision's protections are imposed as contractual commitments does not render them inadequate. Indeed, the EU legislature concluded in the Data Protection Directive (and, more recently, in the GDPR) that contractual commitments *can* adequately protect data transferred to non-adequate jurisdictions so long as data subjects have the ability to enforce those protections and the data importer has an obligation to comply with them. Were the CJEU to require that these safeguards be enshrined in the *law* of the third country, it would nullify Article 26 by holding that transfers may take place only under Article 25 (i.e. if the Commission has determined a third country's legal regime to be adequate).

49. The EU legislature determined that the SCCs must include several specific safeguards in recognition of the fact that data importers could be subject to domestic legislation that would override their contractual commitments. As described in paragraph 32, for example, the SCCs require that a data importer: (i) warrant that any applicable third-country legislation will not prevent it from fulfilling its obligations under the SCCs; and (ii) notify the data exporter if any legislative change is likely to substantially adversely affect its ability to comply with these obligations. In such cases, the data exporter can terminate the transfers.[38] This mechanism allows the importer to evaluate the risk that a third-country law will interfere with its contractual commitments. This mechanism also ensures that, to the extent a domestic law is incompatible with an importer's SCC commitments, the exporter can cease transfers of personal data to that importer.

50. The SCCs further provide, as described in paragraph 33, that obligations under third-country laws will not breach the SCCs to the extent they stem from "mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society . . . ."[39] The European Commission adopted this provision – which mirrors the derogation under the Data Protection Directive

[38] *See* SCC Decision, Clause 5(b).

[39] *Ibid.*, Clause 5, footnote 1.

and the Charter, among other European instruments – specifically to ensure that, to the extent a third country law imposes obligations that contravene the SCCs, these obligations may not reach any further than what would be permissible under the Charter, the Data Protection Directive, and CJEU precedent.

51. In other words, if an importer breaches an obligation under the SCCs in order to comply with a mandatory legal obligation imposed by the law of the country of destination, that is permissible only to the extent that the obligation does not go beyond what is necessary and proportionate to meet objectives of general interest recognised in the Union. To the extent that an importer breaches the SCCs in compliance with a demand that exceeds this scope, the transfer would be impermissible and the supervisory authority may ban it under Article 28 of the Data Protection Directive and the data subject concerned would have a right to damages.

52. Question 8 asks whether, where a Member State supervisory authority concludes that the surveillance laws in the country of import do not satisfy the requirements of the SCC Decision, that authority is required to prohibit or suspend related data flows.

53. We believe that Member State supervisory authorities have discretion to suspend data flows, but are not required to do so in all cases. Instead, a supervisory authority would need to consider the totality of the circumstances surrounding the transfer – including the level of risk of foreign governmental interference among other factors – to determine whether "adequate safeguards" had nonetheless been afforded. This is consistent with the CJEU's Judgment in *Schrems I,*[40] and with the SCC Decision, which acknowledge that supervisory authorities retain the full powers conferred on them pursuant to Article 28 of the Data Protection Directive. Article 28(3) of the Directive, in turn, confers upon supervisory authorities "investigative powers" and "effective powers of intervention." It does not mandate that they exercise such powers, however.

[40] *Schrems I,* paragraph 53 (". . . a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 . . . cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.").

54. EU legislators have also reinforced this conclusion in the GDPR. Article 78 of the GDPR provides data subjects with a remedy in cases in which a supervisory authority chooses not to act, or acts in a way that the data subject believes is inconsistent with his or her fundamental rights. By providing this remedy, the GDPR makes clear that: (i) supervisory authorities *do* have discretion, but that (ii) to fully protect the rights of data subjects, that discretion is ultimately subject to judicial review.

55. Finally, question 11 asks whether the SCC Decision violates Articles 7, 8 and / or 47 of the Charter.

56. The answer to question 11 is "no." The SCC Decision and the SCCs impose safeguards adequate to protect the fundamental rights of EU data subjects, and to ensure that they are afforded a meaningful judicial remedy if those rights are violated, as we have detailed in paragraphs 30-36. In effect, these obligations ensure that the protections enshrined in the Data Protection Directive travel with data transferred under the SCCs. Further, the derogations to the SCCs, for example, to safeguard national security, are not broader than under the Data Protection Directive itself; to the contrary, as explained in paragraph 33, the SCC Decision mirrors the Data Protection Directive in this regard.

VI. Conclusion

57. BSA therefore respectfully proposes that the Court of Justice of the European Union reply to the questions by the referring Judge as follows:

Question 6

In assessing the level of protection to be afforded to personal data transferred to a third country pursuant to Commission Decision 2010/87/EU, OJ L 39, as amended, a national supervisory authority must consider whether the protections afforded by that Decision, along with any other measures adduced by the controller, provide "adequate safeguards" with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Directive 95/46/EC. This assessment in turn requires consideration of the complete set of circumstances surrounding the transfer involved – circumstances that include, among others, the type of data involved, the purposes

of the processing, and safeguards adduced by the controller and importer to protect the transferred personal data.

Question 7

The fact that the protections afforded to personal data and to EU data subjects in Decision 2010/87/EU, OJ L 39, as amended are contractual in nature does not preclude the Decision from affording "adequate safeguards" within the meaning of Article 26(2) of Directive 95/46/EC.

Question 8

Pursuant to Article 28(3) of Directive 95/46/EC, Member State supervisory authorities are vested with the power to investigate and, if appropriate, block transfers of personal data, including transfers made pursuant to Commission Decision 2010/87/EU, OJ L 39, as amended. Consistent with that Article and Court of Justice precedent, exercise of that power is discretionary.

Question 11

Commission Decision 2010/87/EU, OJ L 39, as amended, does not violate Articles 7, 8 or 47 of the EU Charter of Fundamental Rights.

58. Should the Court conclude that despite the above, the SCC Decision must be invalidated – a decision with which we would respectfully and vigorously disagree – we encourage it: (i) to limit the effect of its judgment so that it applies prospectively only;[41] and (ii) to provide guidance sufficient to allow the European Commission to redraft the SCC Decision in a manner that complies with EU law (which the Commission must do in any case to align the SCCs with the GDPR).

[41] The CJEU has made clear that it can limit application of its judgment if there is "a risk of serious economic repercussions owing in particular to the large number of legal relationships entered into in good faith on the basis of rules considered to be validly in force" – a test that we would argue is met in this case. *See,* e.g. *Forposta SA v Poczta Polska SA,* Case C-465/11, EU:C:2012:801, paragraph 45.

September 20, 2018

For BSA | The Software Alliance

Its counsel,

Bart Van Vooren and Kristof Van Quathem

VII. SCHEDULE OF ANNEXES

			Page Numbers within Annex Series	Page Reference in Procedural Document (footnote/paragraph)
A.1	**Annexes related to BSA documents supporting the SCC Decision**			
	A.1.1	Survey of The Software Alliance and U.S. Chamber of Commerce Members: C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") Referral Questionnaire Responses	1 - 2	p. 5 (fn. 6)
B.1	**Annexes related to documents from the legislative history of Directive 96/46/EC**			
	B.1.1	Council Outcome of Proceedings of Working Party on Economic Questions (Data Protection) on 23 and 24 July 1991, 7767/91, July 31 1991, pp. 13-15	3 - 21	p. 8 (fn. 15)