Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Comments on draft EDPB Recommendations on supplementary measures

CCIA appreciates the opportunity to comment on the European Data Protection Board's ("EDPB") draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("the Recommendations").

The Recommendations establish a step-by-step methodology that is a helpful framework for companies assessing their data transfers. However, compliance with the Recommendations as currently formulated would place an unprecedented burden on European and international companies and depart from the GDPR's risk-based approach to data protection. Above all, the collective impact of the Recommendations would prevent the majority of data transfers outside the EEA resulting in significant economic and social drawbacks without corresponding benefits in the protection of European citizens' data.

Our comments raise specific considerations for ensuring that the Recommendations provide pragmatic, practical guidance for organisations in evaluating and securing their data transfers as required by the GDPR and articulated by the CJEU's judgment in Schrems II. *We further encourage the EDPB to carefully consider this consultation in developing final guidance on supplementary measures and to ensure that organisations transferring data have appropriate flexibility to confidently conduct transfer assessments and implement any appropriate safeguards. For additional comments and suggestions on data transfers generally, we refer you to CCIA's paper on Ensuring Secure Data Transfers post 'Schrems II' sent to the EDPB on 27 October 2020.*

The Recommendations create significant, undue data transfer restrictions

Organisations of all sizes and in all sectors rely on Standard Contractual Clauses ("SCCs") to conduct routine transfers of information for a wide array of purposes including engaging with customers, securely processing information, and expanding global supply chains. CCIA strongly supports the goals of the European data protection regime and the need to ensure that European citizens' fundamental rights are protected when their personal information travels overseas. However, as presently formulated, the collective impact of the Recommendations threatens to prevent the majority of data transfers outside the EEA by rendering SCCs virtually worthless for the vast

majority of transfers.[1] The potential negative effects on EU economic competitiveness, innovation, and society are profound and without precedent. Further, these restrictions would threaten to disproportionately jeopardize additional fundamental rights such as expression, information and the freedom to conduct a business.[2]

Inconsistent with the Court of Justice of the European Union's (CJEU) recent judgment in case C-311/18 ("*Schrems II*"), the Recommendations threaten to effectively prohibit reliance on SCCs to transfer data to non-adequate jurisdictions for three primary reasons.[3] First, the Recommendations introduce onerous compliance obligations in assessing foreign laws and practices that, without further guidance, are likely to disproportionately and prohibitively burden SMEs. Second, the Recommendations point to an incomplete formulation of "European essential guarantees", appear to disregard the GDPR's risk-based approach to data protection, and articulate standards that most countries, including those in the European Union, would be unable to meet. Third, the Recommendations recognise only narrow, highly prescriptive technical supplementary measures that are inconsistent with practical requirements for conducting routine business practices in the modern economy. Consequently, the Recommendations will confront organisations with a choice between continuing to trade and use services supplied by non-EEA businesses (risking GDPR fines irrespective of whether disproportionate access to data occurs), or severing trading relationships that will foreclose market opportunities, disrupt routine business practices, and force companies to adopt less secure and reliable service alternatives.

CCIA invites the EDPB, the European Commission and the Member States to reflect on the pragmatic and economic consequences of a rigid interpretation of the *Schrems II* ruling, particularly at a time of economic crisis. In the words of former EDPS Peter Hustinx, European data protection law is intended to encompass a "reasonable degree of pragmatism in order to allow interaction with other parts of the world."[4] As such, CCIA cautions against establishing inflexible guidance that is

[1] See e.g., IAPP-EY Annual Privacy Governance Report 2019, finding SCCs to be the most commonly relied upon instruments extraterritorial data transfers, used by 88% of survey respondents, *available at* https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

[2] See, Recital 4, GDPR; Articles 7, 11, and 16 Charter of Fundamental Rights.

[3] Court of Justice of the European Union, Case C-311/18 "Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems" (16 July 2020), at ¶ 149, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN.

[4] Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation," (14 Sept. 2015) at 49, *available at* https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

functionally incapable of exports, and provides the below suggestions to help ensure that the Recommendations enable organisations to transfer data securely and fully consistent with both the GDPR and the CJEU's *Schrems II* judgement.

Foreign laws and practices assessment: an unprecedented burden that could lead to significant compliance inconsistencies

The Recommendations set out a six-step roadmap for data exporters to review their transfers and implement supplementary measures that encompasses multiple complex analyses of legal, factual, and technical issues. While these steps contain helpful guidance for organizations in assessing their data transfers, CCIA recommends that the Board expressly recognise that for many organisations conducting risk assessments and updating data transfer agreements on a case-by-case basis will necessarily require extended review to reach a decision on continuing a transfer. CCIA further suggests that the Recommendations include enforcement guidance encouraging supervisory authorities to grant sufficient time and engage with data exporters to find workable and acceptable safeguards where they believe a transfer does not comply with EU law. Finally, CCIA suggests that the final Recommendations support a consistent and predictable enforcement framework across jurisdictions for accountable stakeholders by clarifying a scalable application of GDPR Article 58(2) measures in response to potential concerns and by framing the level of fines in advance of enforcement actions.[5] This approach will encourage accountable exporting organisations to carefully complete their assessments and take all necessary steps to effectively implement appropriate safeguards.

The Recommendations contain a particularly burdensome requirement in step 3, which instructs organisations to assess whether foreign government and law enforcement data access rules and practices meet EU's privacy and proportionality standards as applied to the specific circumstances of every proposed data transfer.[6] Such assessments require in-depth knowledge of third country surveillance laws and practice and routinely take years to complete in the context of European Commission adequacy decisions. Ultimately, companies are not, and will never be, in a position to

[5] CCIA invites the EDPB to complement Opinion on administrative fines (wp253) with common minimum guidance on: (a) appropriate safeguards during investigative and corrective proceedings, including the public disclosure of decisions, (b) the methodology determining when corrective sanctions are sufficient to address an infringement or if a fine should be levied on controllers and/or processors, and (c) a clear process to assess the amount of a proportionate and dissuasive fine in the event corrective sanctions do not sufficiently address the gravity of the infringement.

[6] Sections 30-44 of Recommendations 01/2020.

identify and assess which laws in the country(ies) of destination would fail to meet the EU's proportionality and necessity test and this requirement will necessitate the retention of outside counsel with multi-jurisdictional expertise.

Where the retention of counsel poses a prohibitively expensive obstacle, particularly for SMEs, conducting these assessments on an individual basis would inevitably lead to different findings for the same jurisdictions. Such compliance fragmentation would be further aggravated if organisations and counsel rely on an incomplete EDPB assessment of U.S. laws and practices and a partial outline of the recent CJEU case-law on serious interferences with individuals' rights in the context of national security, such as is the case in Recommendations 01/2020 and 02/2020.[7]

CCIA encourages the EDPB to develop final Recommendations that support consistent application and enforcement of the data protection rules for cross-border transfers. While the CJEU was clear that it is the ultimate responsibility of the data exporter to ensure that EU data protection standards travel with the data, the CJEU does not prohibit the Commission or the EDPB from assisting data exporters in this endeavour. CCIA believes that the European Commission, in consultation with the EDPB, has a crucial role to play by issuing uniform, country-level guidance on data access laws and practices in order to ensure a harmonized approach to data transfers to non-adequate jurisdictions that provides consistent protections for the data of European citizens.[8] Such guidance would be of significant value to companies in scrutinising their own data transfers to these jurisdictions in accordance with step 3 of the Recommendations. The European Commission has the institutional credibility and the expertise in carrying out evaluations of third-country government data access laws, as is the case in the context of adequacy determinations.

[7] For example, Recommendations 01/2020 do not take into account the significant ways that U.S. surveillance laws and practices have evolved since 2016. Furthermore, Recommendations 02/2020 do not fully take into account the recent CJEU case-law that confirms that national security can justify serious interference with individuals' rights, including the caveats in joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others. This includes elusive language that may exclude recent case-law from the essential equivalence assessment simply because the case referred to Member State laws, not third country laws.

[8] *See* CCIA's paper on Ensuring Secure Data Transfers post 'Schrems II', sent to the EDPB on 27 October 2020, *available at* https://www.ccianet.org/wp-content/uploads/2020/10/2020-10-27-CCIA-Comments-to-European-Commission-and-EDPB-on-Ensuring-Data-Transfers-post-Schrems-II.pdf ("CCIA White Paper").

The Recommendations should incorporate the GDPR's risk-based approach into guidance for organisations' data transfer assessments

Since coming into effect, the General Data Protection Regulation has been recognised and celebrated for employing a risk-based approach to the protection of personal information.[9] This balanced approach ensures that the GDPR serves to maximise the potential benefits of data-driven processing and innovation to individuals, minimising the likelihood of negative impacts to individuals' rights and freedoms.[10] The risk-based approach extends to the context of international data transfers, where the focus is on selecting appropriate safeguards to ensure that the protection of personal information of Europeans is "essentially equivalent" as it would in Europe.[11]

Unfortunately, the Recommendations appear to suggest a departure from this risk-based approach and threaten to introduce a level of inflexibility in organisations' data transfer assessments that is neither required by the Court nor justified by any increase in protection of personal data. Specifically, the Recommendations dismiss consideration of so-called "subjective" circumstances of a transfer such as "the likelihood of public authorities' access to your data in a manner not in line with EU standards" (Para. 42). This approach to data transfer assessments would in effect impose the same requirements on organisations' transfers regardless of the likelihood of the risks for the data subject. This uniform approach to mitigating risk (including in cases of only theoretical risk) is inconsistent with the intent of the CJEU and underlying data protection law as evidenced below:

- The General Data Protection Regulation instructs organisations to take into account the "likelihood" of risks of interference to rights and freedoms when implementing data protection measures.[12]

[9] See e.g., Article 29 17EN WP 248 rev.01 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679."
[10] See Centre for Information Policy Leadership, "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR" p. 13 (21 Dec. 2016), www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/12/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.
[11] *Schrems II* para. 105.
[12] See General Data Protection Regulation Art. 24, 25, 32, 34.

- Commission decision 2010/87/EU on Standard Contractual Clauses for transfer of personal data to processors in third countries includes an assessment of the "substantial likelihood" that the SCC cannot be complied with.[13]

- CJEU's judgment in *Schrems II* emphasized that the legality of a transfer should be assessed on a "case-by-case basis" in light of "all the circumstances of the transfer."[14]

- The EDPB's July FAQs document reiterates the CJEU's judgment that supplementary measures should be "provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country."[15]

- The European Commission's November decision establishing new SCCs encourages parties to a transfer to take due account of the "specific circumstances of the transfer," including "any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred."[16]

- The Recommendations also recognise and encourage consideration of inherently contextual and risk-based factors such as the "nature of the data" and "*possibility* that the data may be subject to onward transfers" (emphasis added) when considering appropriate supplementary measures.[17]

Therefore, in line with the core principles of data protection law and the practical necessity to enable secure flows of data for economic, scientific, and individual purposes, CCIA encourages the EDPB to issue final recommendations affirming that all the circumstances of a transfer are relevant to assessing risk, including contextual factors such as the likelihood of disproportionate access. As CCIA has noted, this analysis should include an array of factors such potential relevance of the data to law

[13] 2010/27/EU (5 Feb. 2010) at Article 4(1)(c) and Clause 5b available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087
[14] *Schrems II* para. 134, 146.
[15] European Data Protection Board, "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*" (23 July 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.
[16] Commission Implementing Decision on Standard Contractual Clauses, Ref. Ares(2020)6654686 (11 Nov. 2020), Annex Clause 2(b)(i).
[17] Recommendations 01/2020 para. 49.

enforcement agencies, volume and category of the data at issues, and whether receiving parties have received prior data access requests from government bodies.[18]

Ensure supplementary measures are outcome-oriented and pragmatic

CCIA welcomes the EDPB's approach to developing a non-comprehensive 'toolkit' of possible supplementary measures that are proportionate according to the GDPR risk-based approach, and that may be used to guarantee that transfers pursuant to SCCs receive essential equivalent protections.[19] CCIA recommends that in developing final guidance the Board consider modifications to ensure that (1) parties to a transfer are free to use supplementary measures as appropriate to ensure essentially equivalent protections for data, and (2) guidance on technical measures is outcome-oriented and of practical use for parties to a transfer.

The Recommendations appear to suggest that technical measures may be required where a foreign law creates the possibility of disproportionate access even in situations where assurances for the security of data could be provided for through other means.[20] Such a requirement would represent a departure from the GDPR and the *Schrems II* ruling, which are neutral as to the form that "appropriate" safeguards shall take and instead focus on ensuring that transfers pursuant to Article 46 mechanisms provide for essentially equivalent protections.[21] This position was further recognised in the EDPB's FAQs, which discuss the development and application potential supplementary measures without regard to "*whether* legal, technical or organisational."[22] Therefore, CCIA urges the EDPB to specify that the adoption of appropriate supplementary measures is outcome-oriented for the protection of personal data, with no inherent hierarchy between the various categories of supplementary measures.

The specific guidance of the Recommendations on technical measures contains highly prescriptive instructions that appear out of sync with technical and practical realities for organisations, and may be outdated as technology continues to evolve. CCIA recommends that the Board's Recommendations adopt a proportionate, technology-neutral approach to supplementary technical measures by establishing clear technical requirements specifying the types of threats that an

[18] CCIA White Paper.
[19] Recommendations 01/2020 para. 70.
[20] Recommendations 01/2020 Para. 48.
[21] See e.g., GDPR Recital 109; *Schrems II* para. 121, 146.
[22] EDPB *supra* note 15 at 5.

organisation should protect against for each category of data. This will ensure that guidance is practical and future-proof for enabling secure data transfers given the evolving nature of security technologies.

CCIA supports strong encryption as a tool that can enable secure data transfers in many contexts.[23] However, the specific guidance of the Recommendations on encryption as a supplementary measure should be modified to reflect practical realities. For example, the Recommendations suggest that encryption will be a sufficient supplementary measure only if it is "flawlessly implemented," which is not a clear or generally recognised concept in the cybersecurity community.[24] Further, the Recommendations suggest that encryption will almost never provide sufficient protection unless the data can never be accessed "in the clear" in a third country.[25] However, preventing such availability of data in a third country through encryption would render SCCs impractical as a data transfer mechanism by foreclosing many routine business practices (e.g. the ability to search, index or automatically process data) and services that require access to the data at some stage to operate. Further, the guidance does not appear to consider a number of existing viable and proven practices such as the use of administrative pre-authorisation controls or the use of automated scripts to perform administrative action on personal data, whereby the scripts can perform restricted actions without any actual human access.

To avoid these consequences, the Recommendations should be revised to ensure that the proposed technical measures are workable and fit for purpose in practice, and that data exporters are able to choose between contractual, organisational, and additional technical measures or a combination thereof, provided that they can demonstrate these controls adequately protect data subjects rights.

Additional Comments to Ensure that the Recommendations are Consistent with GDPR

CCIA agrees with the EDPB that data exporters should "know [their] transfers" (step 1). This is a prerequisite for any subsequent assessment and ensures an equivalent level of protection throughout the processing lifecycle. However, CCIA is concerned that the Recommendations appear to misconstruct the data minimisation principle when it reads: "[y]ou must also verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for

[23] CCIA White Paper.
[24] Recommendations 01/2020 para. 79.
[25] Recommendations 01/2020 para. 88-89.

which it is transferred to and processed in the third country".[26] The data minimisation principle considers the "adequate, relevant, and limited" amount of data in relation to a processing purpose, but not in relation to every processing stage for that purpose. If a transfer is part of a processing operation undertaken for a specific purpose, the data minimisation is met and there is no test under the purpose limitation principle that is focused on that transfer and separate from the other processing activities.

CCIA also remains concerned with the overly restrictive EDPB interpretation of Article 49 as possible grounds to transfer personal data outside the EEA. When the CJEU struck down EU-U.S. Privacy Shield, it argued in paragraph 202 that it is "appropriate" to do so since the derogations in Article 49 prevent "a legal vacuum" that would mitigate the "effects" of the invalidation of an adequacy decision. While the Court recognises that these derogations have their own conditions, it implies that individuals' consent or contract with a company or any other derogations is "appropriate" and therefore capable of replacing an adequacy decision that supports today's massive data flows between the EU and the U.S. or any other jurisdiction. This stands in stark contrast with existing EDPB guidelines 2/2018 (25 May 2018). The frequency and exceptional nature of the transfer varies from one ground to another in Article 49(1) and its subparagraph. Similarly, Recital 111 differentiates between these derogations: "contract" and the "legal claims" derogations are limited to "occasional" transfers, while the "explicit consent", "important reasons of public interest", the "vital interests" and the "register" derogations are not subject to such limitations.

***

For further information, please contact:
Alexandre Roure, Senior Manager, Public Policy, CCIA: aroure@ccianet.org
Keir Lamont, Policy Counsel, CCIA: klamont@ccianet.org

[26] Recommendations 01/2020 para. 11.