The EDPB Recommendations on International Transfers Present New Obstacles for Multinational Businesses and the Global Digital Economy

NOVEMBER 2020

PREPARED BY:

Amy Lewis
alewis@thinkbrg.com
+1 314.276.0736

INTELLIGENCE THAT WORKS

BRG

Copyright ©2020 by Berkeley Research Group, LLC. Except as may be expressly provided elsewhere in this publication, permission is hereby granted to produce and distribute copies of individual works from this publication for nonprofit educational purposes, provided that the author, source, and copyright notice are included on each copy. This permission is in addition to rights of reproduction granted under Sections 107, 108, and other provisions of the US Copyright Act and its amendments.

Disclaimer: The opinions expressed in this publication are those of the individual authors and do not represent the opinions of BRG or its other employees and affiliates. The information provided in the publication is not intended to and does not render legal, accounting, tax, or other professional advice or services, and no client relationship is established with BRG by making any information available in this publication, or from you transmitting an email or other message to us. None of the information contained herein should be used as a substitute for consultation with competent advisors.

The European Data Protection Board ("EDPB") has released a draft for public comment of its long-awaited recommendations on international transfers of personal data in light of the Court of Justice of the European Union's ("CJEU") *Schrems II* decision this past July.[1] The EDPB released these recommendations in an effort to provide guidance for companies uncertain about the legality of their international personal data transfers in the face of potentially severe penalties for noncompliance – up to 4% of annual global revenue or 20 million Euros, whichever is higher. The guidance is being both praised for its thorough examination of the complex legal issues surrounding ongoing international transfers under the European Union General Data Protection Regulation ("GDPR") as well as condemned for its purported disconnect with the reality of the global digital economy and the functioning of multinational businesses.

Under the recommendations, "data exporters" (the companies sending personal data from Europe to a third country) must revisit and assess the legality of each of their international data transfers. Exporters are now responsible for performing a thorough legal analysis of the data protection standards in each country that will receive the personal data, including those countries' national security and surveillance laws, to assess whether those laws allow for the protection of personal data in a manner "essentially equivalent" to the protections in Europe. Companies must consider the lawfulness of international transfers of European resident personal data in common multinational business processes like human resources management, travel and reimbursement, and online activities.

In a November 17 webinar discussing these recommendations, the Secretariat of the EDPB confirmed that data exporters must conduct these analyses even if those transfers are already covered under otherwise GDPR compliant Standard Contractual Clauses ("SCCs" or "Clauses") or Binding Corporate Rules ("BCRs").[2]

Companies must supplement any shortcomings with additional measures to protect the European individuals' right to the protection of their personal data. Because the exporters have the burden of proving that these additional measures are legally sufficient, they are advised to thoroughly document their assessments and supplementary protective measures for each of their international transfers.[3]

The Secretariat of the EDPB confirmed that data exporters should reassess and potentially supplement each international transfer already protected by the Standard Contractual Clauses or Binding Corporate Rules.

1 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
2 https://www.linkedin.com/video/live/urn:li:ugcPost:6734510375758258176/
3 For guidance on how to conduct and document a risk assessment, see the EDPB Guidance on Data Protection Impact Assessments at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

6

Steps

How Does the EDPB Recommend Companies Analyze their International Transfers?

The EDPB's guidance details six specific steps that data exporters should take to ensure the ongoing protection of the personal data they transfer internationally. These six steps are also summarized in a helpful flowchart that the EDPB released alongside its recommendations. [4]

1. KNOW YOUR TRANSFERS

Data exporters should map how their data flows between countries throughout its life, including transfers to sub-processors and third-party systems or servers. Exporters should also identify scenarios where individuals in other countries will have remote access to the data, as the EDPB's recommendations affirmed that remote access constitutes an international transfer. Mapping these flows is an essential prerequisite step for analyzing the legal circumstances of each transfer.

The EDPB affirmed that even remote access to data electronically stored in Europe constitutes an international transfer.

2. IDENTIFY THE TRANSFER TOOL YOU ARE RELYING ON

Even before the *Schrems II* decision, the GDPR required data exporters to identify one of the listed mechanisms to safeguard the data being transferred: an adequacy decision, Binding Corporate Rules, the Standard Contractual Clauses, data protection clauses approved by a supervisory authority, an approved code of conduct, a certification mechanism, or a derogation for a limited and specific situation.

Transfers to countries with an adequacy decision may continue without change, as can transfers relying on a derogation (e.g., in some limited circumstances, consent of the individual whose data is being transferred).[5] However, transfers relying on any of the other available mechanisms, including Binding Corporate Rules, will need to be evaluated in light of the recipient country's relevant laws and data protection standards.

3. ASSESS WHETHER THE TRANSFER MECHANISM IS EFFECTIVE IN LIGHT OF ALL CIRCUMSTANCES OF THE TRANSFER

Even after adopting a transfer mechanism and its inherent protections, there still may be laws or practices in the recipient countries that could prevent an "essentially equivalent" level of protection to that in Europe. Data exporters are obligated to assess these laws and practices and determine whether any gaps remain that could infringe on Europeans' right to data protection. If the assessment reveals such shortcomings, the exporter and importer should work together to implement supplementary measures to bring the transfer's data protection measures up to essential equivalence.

Companies should examine their Article 30 Record of Processing Activities ("ROPA") to identify each international data transfer from Europe to a third country, determine the legal basis for the transfer, and analyze whether supplementary measures are necessary or whether the transfer is unlawful under the guidance.

4 https://media-exp1.licdn.com/dms/image/C4D22AQFW2LmZEd3qLw/feedshare-shrink_800-alternative/0/1605111258845?e=1608768000&v=beta&t=r3mUga8uaQFMynZBbA4HScHDVHyJmVnEFqetFZGUk5Q

5 Article 49 GDPR

To help with this assessment, the EDPB released the supplementary Recommendations on the European Essential Guarantees for surveillance measures, which lists the elements to be considered when assessing a third country's data protection standards.[6]

The EDPB recommendations contain two critical opinions regarding personal data transfers from the European Economic Area to the U.S. First, the EDPB affirms the CJEU's *Schrems II* decision **that the U.S. does not provide essentially equivalent data protection standards** due to its law enforcement and national security laws (e.g., the USA PATRIOT ACT, the Foreign Intelligence Surveillance Act and the CLOUD Act)[7]. This may mean that most transfers to the U.S. not legitimized by a specific derogation will require some supplementary measures to remain compliant with the GDPR.

Second, when assessing the relevant legal circumstances of the transfer, the EDPB states that **companies should "not rely on subjective factors such as the likelihood of public authorities' access to your data** in a manner not in line with EU standards" (emphasis added). In other words, for transfers to the U.S., the EDPB recommendations confirm that companies should not base their assessments on whether the importer has ever received a FISA warrant, national security letter, or similar access request by a public authority in the past; instead, companies must implement supplementary measures if the importer is merely subject to the relevant national security laws, such as FISA Section 702.

4. IDENTIFY SUPPLEMENTARY MEASURES

Where supplemental measures are required, the data exporter and importer should collaborate to implement additional safeguards to fill the identified gaps. These supplemental measures should be identified on a case-by-case basis and may consist of contractual measures such as supplementary data protection agreements, organizational measures such as internal policies and procedures, and/or technical measures such as encryption and pseudonymization. Annex 2 of the EDPB recommendations lists several supplementary measures for data exporters to consider.[8]

The EDPB cautions organizations that contractual measures alone are unlikely to sufficiently mitigate data protection concerns due to national security and surveillance laws because government agencies, such as the FBI and CIA, are not bound by a contract to which they are not a party.

5. IMPLEMENT SUPPLEMENTARY MEASURES

Once the data exporter and importer(s) identify the appropriate supplementary measures, they must implement them to ensure the additional protections are in place before the transfer begins or resumes.

6. RE-EVALUATE AT APPROPRIATE INTERVALS

Lastly, data exporters should monitor and regularly re-evaluate their international transfers. If any material changes occur that affect the level of data protection afforded to the transfer, the exporter may need to adopt additional supplementary measures or, in some instances, cease the transfer.

6 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
7 USA PATRIOT Act of 2001, Pub. L. No. 107-56, 8 USC Sec.1701 (2001); the FISA Act;50 USC Sec 1801 et. Seq (1978.); the CLOUD Act Pub. L. 115-141, 18 USC Sec. 2713 (2018).
8 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Will the New Standard Contractual Clauses Help?

Only somewhat. On November 12, just two days after the EDPB released its recommendations, the European Commission ("EC") released a draft of the updated Standard Contractual Clauses for public comment. While most organizations were hoping the new Clauses would be a "silver bullet" to overcome the compliance challenges posed by *Schrems II*, the EDPB recommendations quashed that hope. In cases where supplementary measures are necessary due to concerns about public authorities' ability to access personal data for national security or surveillance purposes, there is no means of achieving essential equivalence through purely contractual measures, since the third country's public authorities cannot be bound by a contract to which they are not a party.

The new Clauses may still provide some help since they will obligate the importer to adopt certain data protection measures that necessarily will bring them closer to "essential equivalence." However, exporters will still need to examine each transfer and may need to adopt supplementary measures if any data protection gaps remain.

The new Standard Contractual Clauses will not provide a silver bullet solution in countries with national security or surveillance laws that Europe views as excessive because public authorities cannot be bound by a contract to which they are not a party.

Implications for Multinational Organizations, Cloud Services, and Software as a Service

Annex 2 of the EDPB recommendations analyzes seven common scenarios involving the international transfer of personal data and the supplementary measures that may be effective in filling gaps where they occur. The most controversial of these analyses are Use Cases 6 and 7, which examine cloud services hosting data in a third country and remote access to data by entities in a third country for business purposes, respectively. To the surprise of most in the industry, even "considering the current state of the art," the EDPB is "incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights" if the data is "in the clear," meaning that it is unencrypted or made readable outside of Europe at any point during the transfer.

Organizations that rely on cloud services or provide remote access to entities in third countries should work very closely with their data protection officers, privacy teams, legal and compliance teams, and risk management offices to identify their approach to these common types of data transfers given the EDPB's interpretation here.

The EDPB is "incapable of envisioning an effective technical measure to prevent [cloud services and remote access] from infringing on data subject rights" where local laws potentially allow for "undemocratic" government surveillance.

So, What's Next?

The EDPB's Recommendations are still subject to review and comment until December 21, and the Court of Justice of the European Union and European Commission have yet to release any responses on the recommendations, if they even choose to do so. However, regardless of whether the recommendations undergo substantive changes, data exporters should at least begin mapping their international transfers and documenting the transfer mechanism in place for each so they are ready to perform their assessments when the final recommendations are published.

Whether companies are willing, or even able, to perform such analyses remains to be seen, as does whether there will be any appreciable change in the amount of personal data flowing out of Europe even where companies are unable to find sufficient supplementary measures to fully ensure data protection equivalence.

About the Author

AMY LEWIS, CIPP/E, CIPP/US

alewis@thinkbrg.com | +1 314.276.0736

Amy Lewis is a Managing Consultant with BRG's Data Privacy and Information Governance practices. She helps clients' corporate legal and compliance teams develop comprehensive data privacy and security compliance initiatives to mitigate information-related risk. These programs emphasize meeting the principles underlying most privacy regulations, providing clients the agility to meet new privacy compliance demands as they arise in an evolving legal landscape. Such an approach also focuses on strengthening the human element of information privacy and security, empowering the client's workforce with the tools, knowledge and motivation to assist in achieving compliance and doing the right thing with regards to personal data handling and privacy.

About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next.

THINKBRG.COM