MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGH
SINGAPORE, TOKYO, WASHINGTON, D.

December 16, 2020

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

GLOBAL PRIVACY ALLIANCE
COMMENTS ON THE EDPB RECOMMENDATIONS 01/2020
MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

We write on behalf of the Global Privacy Alliance ("GPA"). We welcome the opportunity to submit comments in connection with the European Data Protection Board ("EDPB") Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Recommendations").

The GPA is comprised of a cross section of global businesses from the aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, pharmaceutical, professional services and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

RECOMMENDATIONS

Overall Comments

We very much appreciate the EDPB's efforts to provide guidance in response to the ECJ ruling in the *Schrems II* case. We recognize the challenges such an undertaking presents and we welcome the opportunity to provide input. In terms of the big picture, in keeping with the risk-based approach set forth in the General Data Protection Regulation ("GDPR"), we recommend that the EDPB's Recommendations should be based upon a risk-based approach to both the process for assessing international data transfers and for implementing supplementary transfer measures.

As currently drafted, the EDPB's Recommendations suggest that certain supplementary measures *must* be implemented in order to transfer any personal data without regard to the sensitivity of the information or, most significantly, the risks to the rights and freedoms of data subjects. This is not in keeping with:

- the proportionality principle and risk-based approach set forth in the General Data Protection Regulation (**GDPR**);
- the ECJ ruling in Schrems II, which requires the exporter and importer of the data to verify, on a *case-by-case basis,* whether the law of the third country ensures an adequate protection of personal data transferred under the Standard Contractual Clauses ("SCCs") and by providing, *where necessary*, additional safeguards (see Schrems II sub 134);
- the ECJ ruling in Schrems II, which requires the Supervisory Authorities (SAs) to suspend or prohibit a transfer pursuant to SCCs if, *in the light of all the circumstances of that transfer*, those clauses cannot be complied with and the protection of the data transferred cannot be ensured by other means (see ECJ Rule 2);
- standard case-law of the ECJ 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* (see case law cited in Schrems II sub 172).

For example, consider a medium-sized company in France that is seeking to develop a product with a company in the US. Consider further that an employee of the French company needs to send an email to the US company as part of the normal course of business and – even if the email does not contain any attachments or other personal information in the body of the email – the email will still always contain the employee's name and contact details (by virtue of the email address and email signature involved). If the transfer mechanism for these transfers are Standard Contractual Clauses ("SCCs"), what would be the supplemental measures that the French company could put in place to protect the personal information of the French employee? While encryption would protect the data in transit, it will not work to protect the data after they are received, because the US company would need the key in order to read the email. Key-coding would not work, because again, the US company would need to know the name of the person sending the email. The EDPB draft guidance suggests in paragraph 48 that contractual and organizational measures alone will generally not be sufficient, even when the company is not the clearly subject to Section 702 FISA or E.O. 12333 orders, the data involved in the transfer are not in any manner sensitive and therefore unlikely to be of interest to, and intercepted by, public authorities. Thus, taking the EDPB draft guidance as written, there are no supplemental measures that could be put in place to legitimize the transfer. We do not believe that the EDPB is suggesting that the proper interpretation of the ECJ opinion is that all emails and sharing of HR data between companies in the EU and companies in the

US should cease. Rather we believe and we recommend that the EDPB make clear that a risk-based approach is appropriate.

Similar to the risk-based prioritization taken by the European Data Protection Supervisor ("EDPS") in relation to European Institutions, we recommend that organizations be permitted to focus first on high risk transfers to third countries, such as those involving either large scale or complex processing operations or processing of special categories of data ("sensitive personal data"), transfers for which there are no established transfer tools, and transfers based on a specific derogation. Most intelligence agencies will not be interested in the typical personal information (whether sensitive or not) that is transmitted by a company. We believe that private sector organizations should be held to the same standard as set out by the EDPS for public sector organizations and both should be treated in a manner consistent with the risk-based approach outlined in the GDPR. In particular, the nature and sensitivity of the personal data involved in a transfer should be considered when deciding the necessary supplemental technical, operational, and/or contractual measures, if any. It is not proportionate to require the same controls for non-sensitive personal data as for sensitive personal data. Nor is it proportionate to require the same controls for data that are highly likely to be targeted for interception as data that are highly unlikely to be. This approach is consistent with Article 32 of the GDPR which requires that controllers consider many factors when implementing security, including "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."

We recommend, therefore, that the Recommendations be revised to reflect this proportionality concept by clearly stating that the process for assessing and implementing supplemental measures should be risk-based and should be prioritized based on the sensitivity of the data involved in the transfer and the likelihood that the data will be intercepted by public authorities. Otherwise, the implementation process will be incredibly disruptive to small, medium, and large businesses in Europe and the rest of the world, particularly at a time when economies are already reeling from the economic fallout of a global pandemic.

We also urge that the Recommendations address how critically important transfers, such as those that are essential to combat criminal activities (e.g., compliance with anti-money laundering statutes as discussed in Use Case #7, or anti-corruption programs) or those used to help develop a vaccine in the middle of a pandemic, or other significant medical treatments (that would benefit all countries including EU member states), can still be carried out in cases where appropriate supplementary measures may not be available.

STEP 1: Know Your Transfers

- The EDPB recommends mapping data transfers outside of the EEA, including "*onward transfers*," transfers from a recipient processor outside of the EEA to a sub-processor in another third country or in the same third country. (page 9, paragraph 10) This runs counter to the way in which contractual relationships operate and adds a new regulatory burden with very little benefit.
- This step should be revised to incorporate a risk-based prioritization approach that permits organizations to assess and categorize their transfers based on the degree of risk. In particular, transfers of sensitive personal data to third countries that are most likely to be intercepted by public authorities should be the initial focus.

STEP 3: Assess Whether the Article 46 GDPR Transfer Tool You Are Relying On Is Effective In Light Of All Circumstances Of The Transfer

- *Risk-based approach.* To assess the effectiveness of the transfer tools, the EDPB recommends conducting the assessment of the laws or practices of recipient third countries pursuant to the equivalence standard for all onward transfers. (page 12, paragraph 32) As discussed above, this assessment should be subject to a risk-based prioritization approach.
- *Assessment of Third Country Laws.* The need for third country laws to be assessed should not be required. If that in fact becomes a requirement, requiring companies to make their own independent assessment of the general laws of each of the third countries to which they transfer data is an enormous, impractical, and inefficient undertaking. (page 14, paragraphs 36, 42, and 43)

  Assessments done at the individual company level are likely to produce widely varying and inconsistent assessments of the legal landscape in those jurisdictions and the safeguards required which will not be helpful for individuals or to regulators. In addition, gathering and assessing third country surveillance laws, such as their scope, legal procedures, and degree of judicial redress available, is extremely difficult because the relevant laws, regulations, and executive orders are frequently complex and require an intricate understanding of the local legal framework and governmental institutions.

  Furthermore, assessing a country's laws is incredibly time-consuming and almost impossible to do expeditiously when faced with a critical business deal. It will slow

down commercial transactions and innovation more broadly at a time of unprecedented economic uncertainty.

We believe, therefore, that it will be much more efficient and consistent for the European Commission, rather than each and every company, to be responsible for conducting these general legal assessments without drawing conclusions with regard to the risk determination which should be done at the company level with respect to the transfers at issue. The European Commission has the experience with assessing a country's laws by virtue of its adequacy assessments and is therefore far better placed to conduct such assessment in close consultation with other stakeholders including industry and NGOs now also in the context of the ECJ case. This approach will yield more meaningful and consistent assessments which organizations can then use to assess their individual data transfers. We note that the EDPS in its guidance (see page 9) has indicated "to start exploring the possibility of joint assessments of the level of protection of personal data afforded in third countries and how these could be coordinated between authorities, controllers and other stakeholders to provide guidance and ensure compliance with Schrems II."

- *Likelihood of Government Access.* The EDPB Recommendations (page 14, paragraph 42) appear to reject companies' ability to factor into their assessments the likelihood that their particular data transfers will be subject to government access:

> "Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors, *and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards.* You should conduct this assessment with due diligence and document it thoroughly, as you will be held accountable to the decision you may take on that basis."

We urge the EDPB to reconsider this approach. Data exporters and data importers should be able to consider the likelihood of government access to their individual company transfers as a relevant factor, based on:

  - not only the legislation of the third country (see citation above), but also the *legal practices* in the third country (see explicitly Schrems II sub 126), such as scope, purpose and objectives of the government powers under the applicable legislation, including regulatory guidance and statements from public

authorities, and any other facts that would indicate how such laws have been interpreted and applied;
- the number of previous government requests received by the company; and
- the nature of the data and data transfer involved.

- *Public Authorities.* The EDPB states that companies should pay specific attention to any relevant laws, in particular laws laying down requirements to disclose personal data to *public authorities* or granting such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision and national security purposes). (page 13, paragraph 36) The term "public authorities" is overly broad and is not in keeping with the ECJ decision in Schrems II which considers relevant the fact whether the personal data are "liable to be processed by the authorities of the third country in question for the purposes of *public security, defence and State security*" (see explicitly Rule 1 of the judgement). Regulated entities such as financial institutions are obligated to share information with their regulators and such sharing, which is not necessarily governed by legislation, has nothing to do with surveillance or intelligence agencies, but rather collection by the government in many cases. We note that also in the EU many public authorities (such as tax authorities, financial services authorities, etc.) have powers to request disclosure of personal data which are considered limited to what is necessary and proportionate in a democratic society. We believe that it cannot be expected of companies to make a full 'essentially equivalent' test for the powers of each and every public authority in the relevant third country and request the EDPB to revert back to the more limited scope.

Annex 2: Examples of Supplemental Measures

- ***Technical Measures: Encryption.*** **(Use Cases #1 and 3)**
  - In Use Cases #1 and #3, the EDPB requires "state of the art" encryption.
  - Consistent with Article 32 of the GDPR, the level and type of encryption, the handling of encryption keys, and other encryption controls should be proportionate to the risk (i.e., the nature of the data, the likelihood of the data being subject to government requests, and the impact if the data are accessed by the government).
    - The need for "state of the art" encryption should be determined by the nature of the data transferred and the level of risk. Imposing a blanket requirement imposes a substantial and unnecessary additional burden on companies with no corresponding benefit.

- A requirement to have companies independently determine whether encryption can withstand cryptanalysis by public authorities at some point in the future and/or the requirement to implement encryption "flawlessly" is overly burdensome and in practice not achievable. (see pages 22-24, paragraphs 79.2, 79.6, and 84.9) "Flawlessly" seems to be too high of a standard, especially in the realm of cybersecurity where even the most sophisticated government agencies have been subject to cyber security incidents. Consistent with Article 32, appropriate tools should be used based on the sensitivity of the data and the risks to the rights and freedoms of individuals.

- A requirement to maintain the encryption key in Europe without regard to the sensitivity of the data being transferred raises a number of concerns. It means the only data that can leave the EU are either data that are key-coded or data that cannot be decrypted once the data get to their destination. The examples provided apply to all personal data. This means then, for example, that a financial institution outside of the EU that is required to do due diligence to fight bribery or money laundering would not be able to obtain a list of the names of the individuals who hold public office in a member state. Similarly a company in the EU would be unable to negotiate and enter into a business agreement with a supplier or customer in the US because the EU company could not send a letter or email or sign a contract that includes a signature (the signature is personal data and paper documents cannot be encrypted or, if it is an electronic document, the party in the US would not be able to decrypt the information in order to know who signed the agreement). We note that the derogations in Article 49 (1) sub (b) and (c) of the GDPR only apply in case the transfer of personal data is necessary for the performance of a contract between the data subject and the controller or where the contract is entered into in the interest of the data subject. Where employees sign contracts, these are entered into on behalf of the company and in the interest of the company, rather than by (or in the interest of) the data subject. In previous WP29/EDPB guidance, it has further been made clear that the legal basis of contractual necessity should be applied restrictively and these type of processing activities cannot be considered to be necessary for the performance of the employment agreement. Similarly, if a European company and a US company are cooperating to develop a vaccine, they would not be able to share information

such as the names or professional credentials relating to the health care providers running the clinical tests or developing the treatment.

- Therefore, depending on the type of data, it may be appropriate to address this issue through contractual or operational controls, rather than always requiring technically that keys are in the possession of the data exporter and/or in the EEA/adequate jurisdiction. In addition, a company should be able to assess the legal abilities for government authorities to force a company to surrender the decryption keys rather than to assume this up front. If a company cannot be compelled to surrender the decryption key, the issue of where the key is kept is much less important.

- ***Scenarios In Which No Effective Measures Could Be Found (Use Cases 6 and 7)***
  - Use Cases 6 and 7 (pages 26-27) discuss two transfer scenarios where no effective supplementary technical measures could be found. However, these scenarios - (1) transfer to cloud services providers or other processors which require access to data in the clear and (2) remote access to data for business purposes – are common scenarios used by myriad companies and organizations. We recommend against invalidating transfers in these scenarios in such an absolute manner, because doing so leaves no room for technological innovation in cybersecurity or privacy enhancing technology nor does it consider the significant economic implications and disruptions that could arise if companies were forced to suspend these types of transfers.
  - Use Case 6 (page 26, paragraph 88) involves the use of a cloud service provider or other processor in a country where the power granted to public authorities goes beyond what is necessary and proportionate in a democratic society. In order to execute the assigned task, the cloud service provider would be required to encrypt the data prior to processing. According to the EDPB, the fact that supplementary measures are taken to encrypt the data in transit and at rest is not sufficient if the cloud service provider needs the cryptographic key to unencrypt the data in order to carry out its assigned tasks. However, there are cases where the likelihood of public authorities wanting access to this data is so small that it would be unreasonable to expect the parties to implement additional measures. For example, an EU-based company might send employee contact details to a third party service provider in the US so that the service provider can create an employee directory (to enable all employees to contact each other). It seems extreme to say that the EU company cannot use a US-

based service provider to perform that service. We urge the EDPB to take a risk-based approach.

- The consideration of whether a particular technical measure (such as encryption) is sufficient in Use Cases 6 and 7 in particular should include the evaluation of other factors in the circumstances of the transfer. Just as the applicable legal context will depend on the transfer circumstances (paragraph 33) (e.g., the transfer purposes, personal data categories, and whether the data are stored versus accessed remotely), it would seem that these circumstances should also influence the analysis of what constitutes an appropriate supplementary mechanism. Use Case 7, for example, seems to indicate that there is no technical mechanism that would allow even business contact information (for example, in a company-wide supplier database or in a database used to fight fraud or money laundering) to be appropriately transferred to certain third countries.

- *Remote Access.* Consistent with our proposed risk-based analysis approach, the EDPB should consider expanding its proposed supplementary measures to include remote access. In certain circumstances, the use of remote access and the ease with which it can be terminated could be an appropriate technical measure that allows a data exporter to quickly cut off the ability of an importer to share data following either notification of a request or, in the case of the EDPB's "Warrant Canary" proposal, when the exporter has not received an order (page 32, paragraph 110).

- *Legal Compliance and Legitimate uses.* In Use Case 7, there are no appropriate supplementary measures identified so it is unclear how personal data could be shared with "inadequate" countries outside of the EEA for the purpose of complying with anti-money laundering statutes, which would create significant risks to financial service companies' ability to combat global financial criminal activity. As drafted, it appears that there are no technical measures that a multijurisdictional organization could put in place to, for example, create a global employee directory or a central repository of signed customer contracts or a list of high achieving employees who are recommended for a bonus or promotion. Indeed, it is unclear how data can be shared with any "inadequate" countries outside of the EEA, for any business processing operation, if there are no supplementary measures available to data exporters to align the legal regimes.

- ***Relationship of Recommendations to Data Exporter's and Data Importer's Role as Controller or Processor for the Personal Data***
    - The supplementary measures proposed are generally agnostic with regard to whether a data exporter or data importer is a controller or processor with regard to the data.
    - We recommend that the EDPB take into consideration a party's role in proposing particular supplementary measures.
- ***Supplementary Measures Relating to Data Subjects Exercising Rights***
    - Currently proposed measures include contractual provisions that: (1) only allow access to personal data transmitted in plain text in the normal course of business with the express or implied consent of the exporter and/or data subject (paragraph 116); (2) require an exporter or importer to notify the data subject of a request or order received from authorities unless prohibited by national regulations or policies (paragraph 118); and (3) requiring an exporter or importer to assist the data subject in exercising his/her rights in the third country (paragraph 120).
    - The GDPR requires service providers to assist controllers with the controllers' compliance obligations. In keeping with this approach, we would not expect, for example, a processor to reach out to an EU data subject to request consent or to assist the data subject in exercising legal rights in the third country. However, a controller (such as a parent company importing data from its subsidiaries) might do so. There also may be other supplementary measures that would be appropriate to consider where the importer is a controller.
- ***Transfers from a Data Exporter Acting as Processor to a Data Importer Controller***
    - The Recommendations as drafted appear to be focused on transfers from an EU controller to an non-EU controller or processor or from an EU processor to an non-EU sub-processor; however, the newly released draft SCCs contemplate a transfer between an EU processor and an non-EU *controller*. This fills a previously-identified gap offering European service providers a legal cross-border transfer mechanism without requiring Binding Corporate Rules for Processors.
    - The steps provided for, though, in the recommendations and the supplementary measures themselves do not account for this unusual relationship. In this case, requiring the EU processor to assess the legal

environment in the third country before transferring a controller's personal data back to their home jurisdiction or adding supplementary measures would be overly burdensome and likely dissuade non-EU companies from engaging EU service providers.

- Further, an EU processor would not expect or want a US company to notify it that the US company received an access request from the US government relating to the US personal data that the EU processor handled at some point.
- Those transfers should be carved out in the recommendations. The draft standard contractual clauses contemplate a situation whereby the EU processor is only processing information received from a controller and not collecting personal data on that controller's behalf and provides for some language or requirements to be excluded. We recommend that the EDPB take a consistent approach in the final Recommendations.

We request the EDPB to clarify how these supplementary measures work or consider different recommendations based on the role of the importer.

Thank you for your consideration.

Sincerely,

Miriam Wugmeister