European Data Protection Board
Rue Wiertz 60
B-1047 Brussels

18 December 2020

(Submitted via email)

Dear EDPB Secretariat,

Standard Chartered's comments on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Standard Chartered appreciates the European Data Protection Board ("**EDPB**") publishing the above Recommendations ("**draft Recommendations**"), which seek to provide clarity to companies on how to continue to make GDPR-compliant data transfers to third countries, in light of the 2020 CJEU Schrems II ruling ("**CJEU ruling**"). We support the Recommendation's aim of ensuring that personal data originating in the EEA carries with it protections which are essentially equivalent to those in the EEA, and we welcome the endeavours of the EDPB to assist companies with this complex task.

As a practical matter, however, placing the burden of determining adequacy on individual companies will raise numerous complications. In the end, this shifting of responsibility from the public sector to the private sector will expose the overall ecosystem for the transfer of personal data outside of the EEA to inconsistent interpretations of law, which in turn could result in (i) limiting the overall ability of European businesses to compete on the global stage and (ii) unfair treatment for EEA customers. We request that the EDPB instead consider centralising the jurisdictional assessment in a public institution, whose analysis is then used by all companies consistently and comprehensively.

Should the Recommendations be adopted as currently constructed, however, we strongly suggest levelling the playing field for companies by providing them with a harmonised and consistent set of tools that can be easily accessed and based on which the analysis can be performed. The tools should at the least include (i) a centralised repository of information; and (ii) a uniform assessment framework.

Below, we provide specific comments for your consideration.

- **Case by case assessment creates undue burden, to the detriment of EU trade:**

  We agree that a comprehensive analysis of all transfers of personal data to third countries is a sensible step. As noted by the EDPB, however, assessing transfers on a case by case basis is a complex task. Indeed, this analysis is an expansive and complex undertaking, requiring extensive time and resource, assuming it is to be (i) done on a case by case basis, and (ii) performed not just in relation to data we transfer, but also in relation to any onward transfer of that data too. We believe this requirement will unintentionally act as a deterrent to trade out of the EU.

Standard Chartered Bank
1 Basinghall Avenue
London EC2V 5DD
Tel +44 (0)20 7885 8888
www.standardchartered.com

Suggestion: Given the lack of visibility of onward transfers available to the vast majority of companies, we suggest the assessment be done in categories of similar types of transfers to the same end-destination jurisdiction, or route of transfer. Regardless of approach, a grace period of at least two years would be necessary to enable companies to adopt the systems and the underpinning analysis needed to adhere to the Recommendations.

- **Adequacy assessments at an organisational level exposes the ecosystem to divergent analysis:**

  The draft Recommendations requires companies to ensure that the laws of the importing third country contain European Essential Guarantees (EEGs). The implication of the requirement is that each individual organisation, in collaboration with the data importer, must (i) make their own determination as to the current level of personal data protection within a third country and (ii) regularly refresh this assessment in case of legal / regulatory / supervisory changes with respect to access to personal data.

  Most companies, both inside and outside the EEA, will not have the requisite level of expertise of the relevant laws and regulations required to conduct such a review, particularly in relation to central government surveillance. More importantly, however, such an approach will by definition be subject to individual interpretations, increasing the likelihood of inconsistent outcomes across companies, sectors, and regions. The most probable result will be unfair outcomes for customers, costly legal disputes and significant inefficiencies for companies operating within the EEA that choose, or need to, transfer personal data outside the EEA.

  Finally, if a given company concludes that the importer country does not meet the EEGs, the expectations as set out by the Recommendations is that the data should be encrypted to such a degree rendering it unusable by the data importer; clearly an impractical outcome.

  Suggestion: We believe establishing a harmonised (standardised) approach is required and recommend amending the Recommendations as necessary.

- **Expertise and capacity limitations in assessing third country's laws:**

  One factor in determining the adequacy of a third country's data protection laws is the extent to which public authorities can access or intercept personal data. In addition to the inconsistency issues, highlighted above, analysing such a body of legal information would be a significant undertaking, proving challenging for even the largest of companies with extensive legal resource.

  Suggestion: Such an assessment must be done by a public body such as the European Commission. Indeed, there is scope and precedent for greater cross-border clarity and cooperation in such areas such as FATF/AML regulation, where a public body helps ascertain countries' compliance with money laundering regulations. In the absence of this, we suggest the European Commission or EDPB develops and maintains a repository of information on third country laws which companies can utilise free of charge. This would make compliance with the draft Recommendations far more manageable for companies, particularly for SMEs with scant legal and compliance resource. It would also reduce the risk of inconsistent and/or low quality jurisdictional risk assessments and potentially poor decision making taken off the back of those risk assessments, which ultimately could place individuals' personal data at risk.

- **Misalignment between the Recommendations, and the proposed new SCCs and GDPR:**

  As currently drafted, the draft Recommendations apply to any transfer of personal data regardless of the risk to the individual when taking account of the circumstances of that transfer including the nature of the data involved, the type of data subject, the type of recipient and the purposes of the processing. This runs counter to the proportionality principle contained within both the GDPR and the proposed new SCCs that have recently been consulted upon.

Suggestion: The data type and data subject should be explicitly included as factors to be considered in risk assessments, to reassure companies that some level of proportionality in the risk assessment is permitted.

- **Inconsistency with EU's Data Strategy objective:**

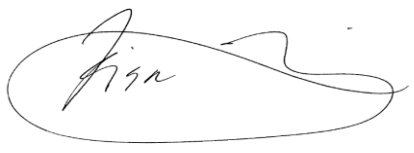
  We welcome the EU's Data Strategy, which was consulted upon earlier this year. We believe that these draft Recommendations, and more generally the lack of a coordinated and practical response from central authorities to the CJEU ruling, run the risk of impeding the EC's objective of creating a single market for data. Not only could jurisdictional risk assessments vary wildly within a Member State, they could also vary significantly across Member States, if there is no centralised authority or centralised coordination around these assessments. Furthermore, if adequacy assessments of third countries are indeed left to individual companies to conduct, we think this could discourage both fledgling companies and mature companies from either setting up in the EEA in the first place, or expanding across borders given the risk and significant burden this decentralised approach poses.

Whilst we have significant concern about individual companies having to take decisions in relation to the adequacy of third countries, if the EDPB wishes to continue on this basis, we would welcome a repository of information accessible to all companies which would make the required risk assessments do-able for a far greater number of companies. In addition, we highlight the significant undertaking that adhering to the Recommendations presents and therefore politely request a grace period of at least two years in order for companies to endeavor to adhere to them.

We note that aspects of the supplementary organisational measures contained within the draft Recommendations provide a helpful starting point for companies to take confidence in terms of the compliance of their data transfers, and we appreciate this.

We would be very pleased to discuss our views in further detail.

Yours Sincerely



Farisa Zarin
Global Head, Group Public & Regulatory Affairs