DANISH CHAMBER OF COMMERCE
Square de Meeûs 22B
B-1050 Bruxelles

www.danskerhverv.dk
info@danskerhverv.dk
T. +32 2218 2320

IT-Branchen

DANSK ERHVERV
Danish Chamber of Commerce

To the EDPB

December 21st, 2020

The Danish Chamber of Commerce contribution to the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

The Danish Chamber of Commerce welcomes the opportunity to provide input to the public consultation on the European data protection Board "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data".

General remarks

Data transfers between the EU and so-called third countries - and the US in particular - are of enormous importance to European companies and the European economy in general. For the same reason, we must therefore *strongly call for a replacement between the EU and the United States for the now illegal Privacy Shield scheme*. In addition*, the work with new adequacy decisions on* countries where data transfers are a common occurrence due to outsourcing of IT and business processing *should be given priority*. The ability of European economies to engage in commerce with customers, suppliers, and partners outside the EU is critical not only to the recovery of the European economy post COVID-19, but also to Europe's and European companies' success in the global economy. Engagement requires typically transfer of personal data.

In the light of the huge data transfers to the US, we can only perceive the guidelines and SCCs as a temporary solution concerning the US. Having said that the Danish Chamber of Commerce certainly welcomes the publication of the draft guidelines from the European Data Protection Board to fill the gap in this interim period until we have a new agreement with the US in place. They are very important and very needed, because most companies right now are on very uncertain ground when transferring data to third countries.

It's essential, however, to find the right balance in these guidelines for European companies, large and small and across every sector, that rely on the ability to transfer personal data outside of Europe every day, while maintaining the highest protection of data subjects. Building on this, the Danish Chamber of Commerce would like to raise the following points and concerns:

The draft recommendations are based on the ruling of the European Court of Justice ("European Court of Justice") in July 2020 in "Schrems II" - but they *go much further than the ruling of the European Court of Justice*, the General Data Protection Regulation (GDPR) itself and seem to suggest the application of *protection measures that are extremely impractical* and will have significant *negative implications for companies, citizens and public authorities across Europe*. In addition, the decision in the Schrems II case is of great concern to European organisations of any size and sector. It is therefore critical that one has waited so long for this consultation. While the EDPB

is consulting on the Recommendations, it has provided only a very short time period for input. However, the Danish Chamber of Commerce was pleased to see that the consultation period has been extended to 21 December 2020. Data flows are an ever-present part of our society and discussion on their future should be given time needed to reach a practicable solution. In addition, the role and value of data flows in everyday life means that all stakeholders should be active courted for views and the spill over impact of rushed decision should be considered.

The Danish Chamber of Commerce endorses strong protections for personal data, including when data is transferred to third countries. But we have substantial concerns about some potential interpretations of the Draft Recommendations. The EU Charter and the GDPR provide important and valuable protections for personal data. Aspects of the EDPB's Draft Recommendations provide helpful guidance in terms of how to ensure those protections are respected in relation to transferred data. Unfortunately, however, other aspects appear to go much further, and suggest *a range of unworkable measures that would block or significantly impair data transfers, with little (if any) added benefit for EU data subjects*. The right to the protection of personal data must be evaluated in relation to its function in society and be balanced relatively to other fundamental rights.

European organisations transfer personal data outside Europe every single day for a wide range of purposes. The draft recommendations, if adopted, will make many of these transfers considerably more expensive, especially for small and medium-sized enterprises and in some cases probably impossible. More specifically, the draft recommendations propose, *firstly*, that organizations transferring personal data to most third countries around the world, should *generally apply supplementary technical measures to protect data, even where there is only a theoretical possibility and very low probability that third country national security authorities can or will obtain access to the data. Secondly*, the Recommendation *proposes technical measures that are cumbersome and impractical, if not impossible, to implement (e.g., isolation of data in the EU, anonymisation or providing encryption keys to unrelated third parties)*. In the case of some transfers, including where data is used "clearly" in the third country, the recommendations suggest that there are cases where such transfers may not be permitted at all - *regardless of the likelihood and seriousness of the risk of the data involved or the nature of the transfer*.

Specific remarks

Re. The Draft Recommendations should be risk-based in-line with GDPR.

Cross-border transfers of personal data are an integral part of the day-to-day operations of most organisations in Europe. Companies in a diverse range of sectors, including healthcare, transport, retail, IT and financial services, as well as public sector bodies, routinely rely on the standard contract clauses ("SCCs") and binding corporate rules ("BCRs") to transfer data. These transfers take many different shapes and forms, involving many different types of data, different processing purposes, and different recipients in different locations. *In many cases, the transferred data is of no conceivable interest to third-country national security authorities, even though it is considered personal identifiable information. The Draft Recommendations don't reflect the importance of the specific circumstances of a transfer*. Instead, they suggest that organisations must adopt further safeguards any time there is even a theoretical possibility that data may be accessed. Because there is a theoretical possibility that data may be accessed almost any time a company uses the Internet

to communicate with people outside the EU, or shares IT functionality with non-EU entities or enables citizens across the world to connect, this means additional safeguards will need to be adopted in almost every business transaction—regardless of the likelihood and seriousness of the risk of access.

RE. The recommendation goes beyond what the GDPR or the European Court of Justice's judgment in Schrems II requires

a) Step 1-6 roadmap

GDPR establishes a risk-based framework for the protection of personal data. The SCCs and other Article 46 transfer mechanisms are also risk-based. In doing so, data exporters must consider which "appropriate safeguards" for a transfer based on the level of risk involved (GDPR Article 46 (1)) may be selected. The European Court of Justice's Schrems II ruling also recognizes that exporters must carry out a "case by case" assessment and that "all the circumstances of the transfer" must be taken into account when deciding whether a transfer can continue (e.g. 121, 126 134[1]).

As a consequence of this judgement the EDPB presents a six-step roadmap, which certainly *places a heavy burden on organisations exporting data and will require significant resources to comply with (and to maintain compliance on an ongoing basis)*. For example, the roadmap requires a detailed analysis of the characteristics of every transfer, an assessment of all applicable local laws (including complex surveillance laws) and how they impact on the requirements under EU law (which in and of itself requires a detailed assessment). This is a *highly complex assessment requiring specialist multi-jurisdictional legal advice which many businesses will not have* otherwise have available to them. *The cost of obtaining that advice will be prohibitively expensive* for many and *we need a much more simple and workable solution, primarily focusing on whether the third country has data protection rules similar to the GDPR and an independent DPA*. It is also *unclear, to which extend the data exporter should document this analysis*. We suggest, that the EDPB presents an informative practical example, how such a documentation could look like.

As already mentioned above, the approach from the EDPB seems to be, that because there is a theoretical possibility that data may be accessed legally from authorities in the third country, this must lead to additional safeguards. Instead of focusing primarily on the legislation in the third country (publicly available or not), *it should be taken more into account how the authority in the import country has acted, or the technical set up which already has been put in place* and the likelihood that the data transferred will be of interest to public authorities outside the EU/EEA. You will also find a more individual approach in the EU Commissions new SCCs, which enshrine a risk-based approach to data transfers and processing in Section II, Clauses 2-3. Clause 2 states, that organizations must take into account 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*".

[1] http://curia.europa.eu/juris/document/document.jsf;jsessionid=CD01F2FB0A27DB9D696E7BC529CA5ABA?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=17791215

If there is not enough room for a case by case assessment we end up with a formalistic "one-sized-fits-all" approach - suggesting that technical measures are always required where there is only a theoretical possibility of public access, regardless of the context of the transfer.

b) Use cases in Annex 2

EDPB provides "Use Cases" that do not recognize that technical security measures may not be necessary for some transfers; that other sufficiently fully audited international standardized technical and organizational security measures are already in place, or even that contractual and organizational guarantees may in some cases be enough on their own.

Therefore, the use cases in *Annex 2 should be replaced with a toolbox of safeguards that exporters can choose among and combine more freely depending on the nature of the transfer*. The proposed approach to safeguards in a size that suits everyone is not practically applicable and it is not necessary. Instead, the draft recommendations should identify a list of potential safeguards but be clear that data exporters should be free to choose the guarantees they deem most appropriate in the light of the transfer.

Re. Safeguards are disproportionate

The draft recommendations not only require the use of safeguards where there is a theoretical possibility that others will have access to the data, but the recommendations go further and state that *organizational and contractual measures are generally not sufficient to overcome public authorities' access to personal data and technical measures are required instead*. The recommendations do *not take into account the context of the transfer and the level of risk and likelihood involved*. In addition, *the proposed technical measures are often practically inapplicable*. E.g.:

- The recommendations indicate that in order to be adequate, technical measures must prevent all public access to data (e.g. point 48), including through encryption of data that is "error-free implemented" and resistant to cryptanalysis (e.g. use case 1). It is unclear how a company can “flawlessly” implement encryption or effectively prevent a foreign government with all its sources and tools from accessing data.
- Furthermore, the proposal that data should always be encrypted at rest with all encryption keys contained exclusively in the EU (or other appropriate jurisdiction) is virtually impossible. Any use of data such as sending emails or texts, processing customer payments or engaging in business partnerships requires that data be available in a decrypted format.
- The recommendations also seem to suggest that it is required to analyse the economic and technical capabilities of foreign intelligence agencies to decrypt or intercept such encryptions; this is by all means an impossible tasks as such information is not publicly available – even inside the EU/EEA

By applying these extreme safeguards to risk-free transfers, the draft recommendations will interrupt many transfers that are low or no risk, and in many cases make transfers impossible altogether, even in cases where data transfer would be hugely beneficial to the data subject, or society more broadly, such as the transfer of health data when they are subject to significant guarantees that are necessary to tackle the global health crisis. *The role of the recommendations should*

not be to prevent the transfers but rather to provide workable guidance to enable them. The European Court Justice's Schrems II ruling also recognizes that additional safeguards do not require an indefinite guarantee that access to data by third parties can never occur. Preferably that the additional safeguards should establish an "effective mechanism that make it possible, in practice, to ensure compliance with the level of protection required by EU law…" (137). However, the Draft Recommendations don't reflect and don't take into account that the safeguards should be assessed by proportionality.

Re. Clarify how a combination of safeguards (technical, contractual, and organisational) can be effective

In some cases, technical safeguards can be the most effective additional safeguards, for example to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, such as to challenge orders when the relevant legal requirements are met. And contractual safeguards can support these measures by imposing liability on data importers to comply. To the extent that the Draft Recommendations can be read to conflict with such an approach, they should be revised.

Finally, *the Danish Chamber of Commerce supports analysing the effects of the measures on the EU and Danish market to constantly improve the effectiveness of the CBAM and ensure that the mechanism does not have any counterproductive side effects*. The Danish Chamber of Commerce will evidently contribute to analysing the effects of the mechanism with reference to the EU and Danish market.

Re. The proposed approach of the EDPB may weaken the protection of EU data subjects.

European companies generate data transfers daily - cross-border data flows are an integral part of today's global economy and society. Which will also continue once the draft recommendations are completed. If the EDPB makes it difficult or impossible for organizations to rely on SCCs (and other measures under Article 46 of the GDPR), *exporters are likely to try instead to rely on the exceptions in Article 49 of the GDPR to transfer data*. Unlike the SCCs and similar mechanisms, the exceptions in *Article 49 contain very limited guarantees. Thus, the draft recommendations may leave EU data subjects with fewer protections than they have today*.

Best regards,

Sven Petersen
Attorney at Law
Danish Chamber of Commerce

Martin Jensen Buch
Senior Consultant
Danish ICT Industry Association

Links:
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Commission-Implementing-Decision-on-standard-contractual-clauses-between-controllers-and-processors-located-in-the-EU