LEWIATAN

Warsaw, 21 December 2020
KL/593/424/ED/2020

The Polish Confederation Lewiatan remarks on "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

We welcome the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the European Union (EU) level of protection of personal data (hereinafter referred to as *the Recommendations*) as it is a crucial issue that will potentialy target future legal frameworks regarding the transfer of EU-US data. We appreciate as well the fact that the deadline of consultation was prolonged, which gives interested stakeholders across all industries an opportunity to provide input.

We would like to indicate the following areas of concerns and make a few initial suggestions to contribute to the public consultation which, from our point of view, should be taken into account and explicitly considered.

1. The overview

The ability to transfer data international is an inherent part of the global economy's operation and social exchanges. In fact, organisations of all sectors within the EU, whether public or private, EU multinationals and SMEs, heavily rely on the possibility to transfer personal data to third countries in order to be able to provide their services in the EU and around the world. Today, practically no organisation, irrespective of sector, would be able to do business, let alone take part in international trade, without the ability to transfer data cross-borders. Data flows play an invisible but structural role in the delivery of products and services that EU citizens rely upon in day-to-day life. *The Recommendations*, if adopted, will force many aspects of EU commerce and society into a pre-internet era, and isolate Europe from the global economy and have potential negative effects on EU competitiveness, innovation, and society are enormous.

The Polish Confederation Lewiatan regrets that the wording of *the Recommendations* fail to have regard to this reality and that the overly burdensome and prescriptive approach it sets out is likely to have very far-reaching negative impacts on the fundamental rights and freedoms of EU citizens and of EU organizations as well as on the EU economy and way of life more generally.

It is also worth mentioning that *The Recommendations* reflect a failure to take into account any of the other rights and freedoms enshrined in the Charter of Fundamental Rights as well as other legitimate interests, including the present and future of the EU economy, the social well-being and health of EU citizens and EU security that requires a global approach.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

The Recommendations are overly prescriptive and place a heavy burden on organisations that may not always have the capability to achieve and maintain compliance. For example, the roadmap requires a detailed analysis of the characteristics of every transfer, an assessment of all applicable local laws - this is a highly complex assessment requiring specialist multi-jurisdictional legal advice, to be routinely re-evaluated, which many businesses will not have available to afford. In addition, the cost of implementing some of the actual recommended safeguards would make many businesses unviable or prohibitively onerous.

Moreover, we strongly believe that *the Recommendations* specifically call for additional supplemental measures that make access impossible or ineffective in the third country. In practice, this would prohibit any EU business from relying on many global service providers that provide communication services (e.g., email, videoconferencing, posts, etc.) or money transfers that must access communications or related personal data to deliver these services. Moreover, a great number of business entities could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question. They also will require EU organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries, which will be unrealistic for most small and medium-sized enterprises, research institutions, and others.

Additionally, the document proposed undermines and will damage EU businesses and EU citizens rights as well as opportunities by failing to adopt a proportionate and risk-based approach and by not acknowledging the importance of other fundamental rights and freedoms, including the right to freedom of expression and information (Articles 11 and 7 of the Charter) and freedom to conduct a business (Article 16 of the Charter). The right to the protection of personal data must co-exist and be balanced against these other fundamental rights.

As of today, we perceive *the Recommendations* more as a list of requirements than helpful guidance for controllers and processors. Instead of a clear reflection of risk assessment, impact assessment and probability analysis in the context of principles relating to processing of personal data and type of transfers, we see *the Recommendations* as a document presenting strict rules applied to every situation. For people in this part of Europe, it reminds ancient regime rule that “everything is forbidden except the things which are clearly allowed”.

From our perspective, by focusing only on non-adequate jurisdictions, *the Recommendations* threaten to create an unequal international playing field for data protection where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them. Such discriminatory treatment of different jurisdictions is also likely to invite retaliation by jurisdictions whose companies are placed at a competitive disadvantage in European markets by the EDPB’s actions.

The Recommendations also ignore the recent CJEU case law that confirms that a Member State national security can justify serious interference with individuals’ rights. *The Recommendations* essentially require organisations to implement specific technical measures in order to rely on the SCCs in many cases and preclude reliance on organisational, contractual and other measures. In doing so, *the Recommendations* depart

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

significantly from the wording of the GDPR and the CJEU Schrems II ruling, neither of which prioritised technical measures over and above other types of measures, such as organisational, contractual or legal.

Furthermore, we would like to express our concern that progress of technology will make *the Requirements* obsolete quickly. As a result, the document proposed will need considerable alterations very soon and finally, will impose additional burden on data processing entities every time the changes will be announced. Some requirements, especially technical requirements, can be impractical and difficult to implement. At the same time, *the Requirements*, if not on the edge of technology, are an easy target for anyone who is interested in limiting or reducing European international trade. It is believed that all businesses these days, internal to EU and international, are digitally supported and data-based.

2. *The Recommendations* should allow data exporters to take account of the full context of a transfer

In Schrems II, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality—specifically, that transfers should be evaluated *"in the light of all the two circumstances of that transfer"* and *"on a case-by-case basis"*. Several passages in *the Recommendations*, however, appear to foreclose this contextual approach. For instance, they state that, if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures. Even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security. Other passages similarly suggest that the likelihood that a public authority will ever access the data is irrelevant.

Restricting transfers of data even where the context shows there is virtually no risk to data subjects will harm every corner of the EU economy and society. EU researchers sharing health data with foreign partners to fight COVID-19, EU companies engaging in routine communications with employees outside the EU, and even simple commercial transactions with non-EU entities would all be fraught with substantial risk. Nothing in the Schrems II judgement requires this draconian outcome. Rather than discouraging EU organisations from considering contextual factors, *the Recommendations* should encourage organisations to take into account the real-worlds risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. If these real-world risks are low, which they are for most categories of data, *the Recommendations* should not require organisations to adopt any supplemental measures.

The EDPB should adopt the risk-based approach of the Schrems II Decision of the ECJ and the corresponding fundamental principle enshrined in the GDPR. The exporter, assisted by the importer, should be able to factor in all relevant subjective or objective criteria to assess the risk of a transfer to a third country on a case-by-case basis. This should include the likelihood of access, interference or request by a foreign government. Likelihood and precedents based on experience cannot be the only factor, but exporter and importer should be able to predict the realistic risk of specific transfers based on prior access requests of public authorities.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

3. *The Recommendations* should propose technical measures that are workable in practice

The Recommendations propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, *the Recommendations*' case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

For instance, *the Recommendations* suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU or an adequate jurisdiction. They also suggest that encryption almost never provides sufficient protection where data is accessible *"in the clear"* in the third country, including where an EU organisation uses an online service that may process the data in the third country, or where employees or others in the third country can access the data on a shared IT system.

Furthermore, because *the Recommendations* state that even remote access by an entity in a third country to data stored in the EU constitutes a *"transfer"*, organisations in many cases would need to apply these technical safeguards to EU-stored data, as well. This fact underscores the impracticality of *the Recommendations* and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests, for instance in the context of the COVID-19 pandemic.

More pragmatically, *the Recommendations*' positions on technical measures would render the SCCs virtually worthless as a transfer mechanism. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information, as *the Recommendations* would require, there is no point to the transfer. Similarly, many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly. Given the nature of the internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. *The Recommendations* would prohibit EU organisations from engaging in these commonplace and essential business activities.

In reality, most EU organisations would not be able to cease these activities entirely while still remaining economically competitive. Instead, many would likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Because organisations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs, to say nothing of additional safeguards, this outcome would leave EU data subjects worse off, because their data would be subject to fewer protections than they are today. However, the EDPB also noted that such derogations, which would include data subject consent, must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

To avoid these consequences, the EDPB should revise *the Recommendations* to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. *The Recommendations* should not prohibit all access to data in the third country. Otherwise, they will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

Taking as an example global cloud service providers, they offer cutting-edge security services, currently protecting sensitive data from attacks by state-of-the-art protection measures. *The Recommendations* could incentivise data controllers to prefer less secure service providers only because of local processing, over those which process data also in third countries to avoid complex risk assessments and monitoring obligations, which would be especially challenging for SMEs. This would considerably lower security standards, which in some cases could have life threatening consequences.

While encryption can provide strong protection against access to data, including extensive data collection by governments, it can only serve as one of several potential measures to protect personal data in transition. The reason is that encryption might impact certain processing activities.

What is more, the general requirement to apply comprehensive encryption to all stages of the data processing would result in companies having to implement very costly encryption methods even cases where the risk is very low. Such encryption measures would be disproportionate, and particularly burdensome for SMEs.

4. *The Recommendations* should clarify that contractual measures may provide sufficient safeguards

Although *the Recommendations* propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organisational measures on their own, for instance, without additional technical measures, cannot provide the level of data protection that EU law requires. This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities, even if the practical risk of such access is vanishingly small, renders a transfer unlawful.

This position adopts an overly restrictive reading of the Schrems II judgement. The Court in Schrems II held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honour them". This language, and similar passages elsewhere in the judgement, suggest that, so long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, that it notifies the data exporter accordingly), then the parties may rely on the SCCs. Under this reading, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the Schrems II judgement, *the Recommendations* should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. *The Recommendations* should instead articulate several possible contractual measures that EU organisations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer".

We strongly recommend focusing on creating valuable recommendations, allowing entities to decide and assess the risks related to data transfers and apply supplemental safeguards accordingly. What is more, the final version of *the Recommendations* should stated as well if and when supplemental safeguards will be

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

implemented as a combination of two or more types of safeguards, which will lead to much stronger protection than applying only one. The "one-size-fits-all" approach is neither appropriate, nor fitting the real needs of small and medium enterprises in Europe.'

The data importer is obliged to include in a contract the procedure and practice of making the data available to authorized government services of third countries. These provisions should function as a basis for assessing the risk referring to access to personal data and the exporter's decision to transfer the data to the country or countries concerned. The importer's proof of actions taken, if known, should be considered as an additional basis for decision making. Such a procedure should be perceived as a sufficient reflection of 'best effort' to assess the legal and practical conditions for assessing personal data protection beyond the SCCs provisions.

5. ***The Recommendations*** **should make clear that enforcement by supervisory authorities will be measured and appropriate**

The Court's holding in Schrems II was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.

Notwithstanding these facts, *the Recommendations* imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with *the Recommendations*. This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices, making it far less likely that organisations address these issues carefully and precisely.

To avoid this outcome, *the Recommendations* should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions. This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues.

Analysing applicable laws in the third country, the compliance dimension will be difficult to achieve. The detailed analysis which seem to be required by the ruling in light of *the Recommendations* goes beyond what can reasonably be expected from companies. The EDPB has highlighted that DPAs will be responsible for enforcing *the Recommendations*. Due to a wide-ranging impact that use cases will have on a vast number of companies, the majority of those in the EU using software and cloud services provided in third countries, including SMEs, but also on almost all multinational companies sharing HR or business client data, DPAs may find themselves in a challenging position that may lead to inconsistent enforcement and compliance and will severely affect the European economy.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

6. Final remarks

In order to ensure that international transfers of personal data can be maintained in a way that guarantees legal certainty and the fundamental rights and freedoms of all EU citizens and organizations, The Polish Confederation Lewiatan urgently call for:

1. The EDPB to understand the need to avoid an overly restrictive approach and to adopt a pragmatic one. It is essential to keep an holistic view in a matter like this one and to balance data protection rights with the economy, scientific research, social well-being, development of other fundamental rights and freedoms and security in the EU.

2. The EDPB works towards enabling transfers rather than prohibiting them.

3. *The Recommendations* to provide practical and workable guidance that will allow for businesses and organisations to take steps to ensure that they can continue to transfer data in a manner which respects the essence of EU data subjects' GDPR rights without ignoring other Charter rights of EU organisations. The EDPB should refrain from including impossible standards such "flawless implementation" of certain safeguards which simply do not reflect the nature of technology or reality.

4. *The Recommendations* to explicitly state that GDPR and the ruling in Schrems II permit reliance on a combination of measures and make clear that there is no hierarchy of measures.

5. The EDPB to align with the European Commission's pragmatic and more realistic approach for the new set of SCCs.

6. The EDPB to recognize that EU and Member States institutions should swiftly negotiate with their United-States counterparts a new mechanism to replace the "Privacy Shield", taking into account all economic and fundamental rights and freedoms, which are not absolute and that the EU and the US share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.

Yours faithfully,

Maciej Witucki
President of the Polish Confederation Lewiatan

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS