Internetconsultation EDPB Recommendation on supplemental measures

The Dutch Confederation of Dutch Industries and employers (VNO-NCW / MKB-Nederland) welcomes the possibility to provide input on the proposed Recommendations on supplemental measures from the EDPB.

We appreciate the effort the EDPB put into drafting the Recommendations on supplemental measures, illustrated with examples, with the aim to provide businesses – in the aftermath of the Schrems-II judgment - with guidance on performing a risk assessment in order to determine which organizational, contractual and/or technical measures to take to supplement the SCCs to mitigate the risks of a specific data transfer to a third country.

Many companies and other organisations, big and small, take part in the global digital economy, an economy that does not recognize borders. As a result of (fast) technological developments and data flows the digital economy will be able to expand in the near future and, for instance, making it possible for SMEs to take their part in the digital economy which is an essential development for their resilience and sustainable development. New European legislation initiatives such as the Digital Services Act and the Data Governance Act have the ambition to empower such growth and strengthen the position of Europe in the global market. Unfortunately the current take by the EDPB in its Recommendations will undermine this singlehandedly. Although the EDPB alludes in its Recommendations to free privacy protected global data flows around the world, close reading of these Recommendation shows us otherwise. Bottom line is that the only usable supplemental measure according to the EDPB are technical measures, namely encryption, pseudonymization and splitting the data and if this fails, no transfer of any personal data is allowed to third countries. Irrespective of the specific risk of actual harm / impact on the data subjects in question. The EDPB is of the opinion that no contractual or organization measures or combination of them can be put into place to enable the data transfer, although the harm / impact on the data subject in question is relatively low. We propose a risk based approach which factors in the specific risk of actual harm / impact on the data subjects in question, taking into account all relevant factors of the data transfer and stay closely aligned with the spirit of the GDPR which fundament is a risk based approach; as well as a holistic view by taking into account other relevant fundamental rights in play. We also propose the EDPB takes an active role in assisting / taking out of hands the assessment of third countries laws. Assessing third country laws is not only too far reaching for most organizations (due to the significant expert resource investment it would take), especially the smaller ones (which would lead to a shift on the level playing field), it will also lead to fragmentation in the internal market which in and of itself does not contribute to increased protecting of the EU citizen's personal data. Last but not least we call for the Recommendations to form a coherent whole with the updated SCCs.

We would like to take this opportunity to address some points of concern regarding the Recommendations on supplemental measures:

Risk based approach

A central feature of the GDPR is its risk based approach. Although the EDPB alludes to the importance of risk (para. 33 and 49), a more explicit recognition of the importance of risk assessments is needed to make the guidance consistent with EU data protection rules.

Under the GDPR controllers need to assess the risks presented to the rights and freedoms of data subjects associated with the processing of personal data to be able to determine which safeguards to apply. The risk based approach also features in the GDPR in order to assess which organizational and technological measures need to be implemented to ensure an adequate protection. The controller needs to take into account the nature, scope, context and purposes of the processing and the risks involved to the rights and freedoms of natural persons (GDPR considerations 74, 75-76; GDPR Article 32, considerations 78 and 83).

The ECJ also underwrites a risk based approach in its Schrems-II judgment. The ECJ is, in our opinion, very clear in its judgment that a case-by-case assessment of the circumstances is needed and that adequate protection can be provided by additional safeguards in addition to the SCCs in the event of lacunae in the law of third countries (recitals 131-134, 146 and 202). The ECJ states in recital 131 of its Schrems-II judgment, the following (IT underlining):

> *131. In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the EU to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject'.*

The ECJ continues in its recitals 132-134 *to state that (IT underlining):*

> *132. Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that 'the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses'.*
>
> *133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.*

> *134 In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.*

The ECJ continues in its recital 146 *to state that (IT underlining):*

> *146. In that context, Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.*

The ECJ continues in its recital 202 *to state that (IT underlining):*

> *As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016, Borealis Polyolefine and Others, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.*

The EC also takes a risk based approach in its updated SCCs[1]. Clause 2 under b states that the assessment can include the likelihood that the government of the third country may have access to the transferred data, whereby the practical experience of the data importer may play a role in the assessment. This is in stark contrast to Recommendation of the EDPB where it states (paragraph 42) that the exporter should 'not rely upon subjective factors as the likelihood of public authorities' access to your data in a manner not in line with EU standards.' The likelihood of access is qualified as 'subjective' which in our opinion is in itself subjective. For paragraph 42 to be more in line with the wording of Clause 2 under b of

[1] Ref. Ares(2020)6654686 - 12/11/2020

the updated SCCs as well as in line with paragraph 43 and 135 of the Recommendations, we suggest to change paragraph 42 as follows (IT bold):

> *42. 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 upon subjective ones.*** *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.*

In addition we suggest to add to paragraph 33 'the likelihood of public authorities' access' to complement the other factors for assessing the circumstances of a particular transfer.

The EC takes more into account than just the third country laws: (i) the specifics of the transfer, e.g. the nature of the personal data transferred etc; (ii) the third country laws including access rights by law enforcement in the third country and (iii) any additional technical and organisational safeguards (see Clause 2.b). Although the EDPB alludes (in paragraphs 33, 43 and 49) to take into account more factors than the third country laws, the bottom line outcome of the Recommendations is quite another. We refer for example to paragraph 52 of the Recommendations where the EDPB states that where a third country prohibits the use of encryption, all personal data cannot be transferred to such a country. This statement in combination with the use cases 1-5 make it apparent that the only usable supplemental measure according to the EDPB is a technical measure, namely encryption, pseudonymization and splitting the data and if this fails, no transfer of any personal data is allowed to such third country. Irrespective of the specific risk of actual harm / impact on the data subjects in question. We also refer to the use cases 6 and 7 which are qualified by the EDPB as scenarios in which no effective measures could be found. These use cases specify the use of cloud services providers or processors which require access to the data in the clear and remote access to data for business purposes (such as remote access from headquarters abroad to HR data on a server of its subsidiary in the EU) irrespective of the particular third country and irrespective of the actual harm / impact on the data subjects with regard to the specific transfer at hand.

The Recommendation of the EDPB seems to suggest that the mere presence of unencrypted or not pseudonymized personal data beyond the borders of the EU can subject it to any manner of intrusion, by lawful or illicit means, by a third country's public authorities (see paragraph 75). The Recommendations essentially boil down to the fact that you can practically only be compliant by either encrypting, splitting personal data or pseudonymizing personal data or by keeping personal data within the EEA (with the exception of countries for which an adequacy decision has been made). We remain united by our vision and commitment for a strong and competitive Europe and we fear Europe cannot remain competitive if localisation of data becomes a widespread practice.

The importance of contractual and organizational measures should not be overlooked. While contractual clauses do not bind third countries' authorities, an importer's commitment to challenge a government request, is an example of a factor to take into account to determine

whether interference will effectively take place. A combination of measures can ensure an essentially equivalent level of protection for data subjects in practice.

A risk-based approach provides data controllers with practical tools to determine how to allocate their resources. To ensure alignment with GDPR, the Recommendations of the EDPB should, in our opinion, stress the risk in terms of impact on the rights and freedoms of the data subjects given the nature of the data and the purpose of the processing, even if they were accessed. This would also be in line with the Article 29 Working Party's "Guidelines on DPIAs and determining whether a processing is likely to result on a High Risk", which the EDPB endorsed. According to these Guidelines DPIAs are only mandatory when the processing is '"*likely to result in a high risk to the rights and freedoms of natural persons, considering the use of new technologies, and taking into account the nature, scope, context and purposes of the processing* (Article 35(1) GDPR)." Exporters should be able to implement more supplemental measures than solely technical measures such as encryption and pseudonymization of personal data, depending on the specific impact on the rights and freedoms of the data subjects given the nature of the data and the purpose of the processing.

We would like to stress the importance of a coherent approach in assessing the risks of data transfers by the EC and the EDPB. The complexity of assessing global surveillance and judicial redress laws is in itself a hurdle to be taken by companies large and small. This puts a lot of pressure on businesses across Europe. Adding a non-risk based approach to this, which does not align with the Schrems-II judgment of the ECJ nor with the risk based approach of the GDPR itself – makes it (fairly) impossible for companies to rely upon SCCs for data transfers to third countries (which do not fall within the scope of the GDPR through article 3).

We would also like to stress the fact that SCCs are the most widely used tool for data transfers and largely recognized and accepted by our counter parties on the external market. SCCs facilitate global trade and research involving personal data processing.

The EDPB recommendations are counterproductive to ongoing adequacy negotiations and the benefits they produce for data subjects globally. The EDPB should leave room for the Commission to drive higher global standards through the ongoing negotiation of adequacy decisions in order to create more robust privacy protections for millions of data subjects around the globe. With the Privacy Shield came reforms to the U.S. surveillance regime and a national data protection law. The possibility of extending adequacy to other countries in Asia, Africa, and Latin America will also raise the bar for data protection.

The Dutch Confederation of Dutch Industries and employers calls for risk based practical EDPB Recommendations on supplemental measures to enable actual use of the SCCs (and BCRs) for data transfers to third countries. As well as ongoing adequacy negotiations to raise the level of protection in the world.

Laborious and expensive task

We would also like to stress that assessing third country legislation is a laborious and expensive task which requires legal knowledge and/or resources for legal counsels which go

far beyond the knowledge and/or resources of most if not all SMEs. Especially as the laws and practices change all the time. We do not want it to be impossible for SMEs to take part in international trade and research projects due to administrative burdens they cannot overcome. The risk of assessing the legal requirements in the country of destination should not be borne by businesses alone.

In our opinion, considering recital 147 of the Schrems-II judgment as well as principles of good governance, article 64(2) of the GDPR provides for the possibility for a supervisory authority to assess the law of third countries with regard to the transfers of data to a third country and to draw up a list of lacunae in the law of such countries and to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision. Such an overview would unburden all companies in the EU, especially SMEs, of the near impossible task of having to assess the law of third countries themselves.

Consistent decisions among DPAs

We would also like to call for emphasis on the need for consistent decisions on data transfer recognized by the ECJ. The ECJ recognized in its Schrems-II judgment that any decision by a supervisory authority to prohibit transfers to a country should be referred to the EDPB for an opinion, "in order to avoid divergent decisions" (Schrems II, recital 147). We suggest the EDPB to explicitly commit in its Recommendations to provide uniform guidance regarding data transfers to third countries.

Jurisdiction-based approach

In its updated SCCs the European Commission addresses the interplay between Article 3 GDPR and chapter V GDPR and opts in article 1.1 (in combination with the wording of recital 7) for a jurisdiction-based approach (instead of a territory-based approach).

We note that the EDPB has so far refrained from explicitly addressing the interplay between Article 3 GDPR and Chapter V GDPR. It stated in its Guidelines on territorial scope[2] that [it] "will also further assess the interplay between the application of the territorial scope of the GDPR as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary." In its recent Guidelines on the concepts of controller and processor[3], the EDPB also didn't provide guidance on the interplay between Article 3 and Chapter V. We welcome the fact that the European Commission has finally addressed the much discussed interplay and has chosen a jurisdiction-based approach. We call upon the EDPB to also explicitly opt in its Recommendations for a jurisdiction-based approach.

On behalf of our members, we appreciate your consideration of our input, and respectfully request that the EDPB addresses these concerns before adopting its final recommendations.

[2] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 22
[3] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, 2 September 2020, considerations 91 (on p. 29) and 116 (on p. 34)

Please do not hesitate to contact us for any additional input or practical examples with regard to any of the issues above.

VNO-NCW / MKB-Nederland
Mrs. Mr I.M. Tempelman
E-mail: tempelman@vnoncw-mkb.nl