**Feedback from NLdigital on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation (Ref. R01/2020 – 11/11-2020)**

Place: Breukelen, the Netherlands
Date: December 21, 2020

NLdigital is the trade association for ICT and telecom companies in the Netherlands. NLdigital represents the industry's interests in dealing with the government and political world. More than 650 companies in the Netherlands are members of NLdigital. Our members range from multinationals to SMEs, from all segments of the industry, making us the foremost advocate and representative of the Dutch digital sector. About eighty percent of our members are small- and medium-sized enterprises (SMEs). The majority of our members process personal data on behalf of their clients as part of their core business and are therefore data processors under the GDPR.

We have developed the 'Data Pro Code', the first (and so far the only) approved Code of Conduct under the GDPR by the Dutch Data Protection Authority (the Dutch DPA). The Data Pro Code is especially designed for SMEs in their role as processor. We all know the discussions and concerns people have surrounding big tech companies, but we should not forget that a large part of processing is performed by SMEs established within the EU. An important addition to the Data Pro Code is a neutral processing agreement, which covers both the responsibilities of the controller and the processor. Large companies can afford to hire lawyers that can draft contracts that comply with the GDPR in detail. Smaller companies do not always have these means. Therefore our Data Pro Code processing agreement is drawn up for them, impartially, so it can be used for the relationship controller – processor but also for the relationship processor – sub processor. A standard processing agreement should fulfil the needs of SMEs as much as, or even more than, the bigger companies. This is why we strongly advocate that the Recommendations published by the EDPB should also take into account the capabilities and resources available of these SMEs.

We welcome the opportunity to provide input on the draft Recommendations and we can see the EDPB has put a lot of effort into these Recommendations. We thank the EDPB for calling for public input into their Recommendations and hope sustained engagement with industry is maintained.

Although we feel that safeguarding the privacy of data subjects is pivotal in the digital economy, the Schrems II ruling has introduced great uncertainty to organisations and put a great burden on the shoulders of multinationals and SMEs of our industry. The EU should remain open, free and connected to international partners. We believe that a risk-based approach is the way to go forward to enable business continuity for the benefit of the EU economy, society and individuals. However, we believe that the crux of the issues raised in Schrems II — i.e., the rules under which government authorities in the US or other third countries can gain access to European data for law enforcement or national security purposes — requires a transatlantic political solution that cannot be fully solved by companies that are grappling with the resulting conflict of laws. We urge all parties involved to work out a solution as soon as possible.

Still, we have some remarks that we would like to point out. In order to ensure that the Recommendations will be viable for SMEs, we call for the Recommendations to provide workable safeguards that will allow for organisations to adopt measures that ensure compliance with the EU level of protection of personal data, while at the same time

NLdigital BV
De Corridor 5
3621 ZA Breukelen
info@nldigital.nl
+31 (0) 348 - 49 36 36
KVK 7167 5574

promoting a thriving global economy in ways that are respectful of the fundamental rights and freedoms of EU individuals. Our remarks are elaborated on here below.

## 1. The draft Recommendations should adopt a risk based approach, in line with the GDPR and the Schrems II ruling of the Court of Justice of the European Union

In Schrems II, the Court stated that when evaluating the legality of data transfers, the full context of the transfer should be considered.[1] Data transfers take many different shapes and forms, involving many different types of data, different processing purposes, and different recipients in different locations. However, several sections in the Recommendations seem to rule out this contextual approach.[2] This prevents organisations from taking a risk-based approach to data transfers, which means that, according to the Recommendations, all data is treated equally. This goes against the GDPR and the Schrems II ruling itself.[3] Furthermore, this runs counter to the Standard Contractual Clauses published by the European Commission.[4] The Recommendations should encourage organisations to take into account the actual risks of data transfers and adopt a risk based approach. When assessing the risk, amongst others, the likelihood of access, interference or request by a foreign government must be taken into account. As the current application of the recommendations may restrict transfers in many cases where a transfer of data to a third country may involve no meaningful risk to data subjects, we encourage the EDPB to eliminate this contradiction.

## 2. The safeguards proposed in the draft Recommendations should remain proportionate

When assessing which safeguards are 'proportionate', 'all circumstances of the transfer' should be taken into account. Nevertheless, the draft Recommendations could be read to take a 'one-size-fits-all' approach. They are quite prescriptive and place a heavy burden on SMEs, that may not always have the capability to achieve and maintain compliance. For example, assessing all applicable local laws requires a detailed analysis of the characteristics of every transfer, which calls for a thorough, multi-jurisdictional legal and technical examination. This should also be monitored and routinely re-evaluated. Many organisations, especially SMEs, will not have the resources available for this nor the ability to incorporate the costs thereof in their services.

Furthermore, requiring this kind of assessment prior to the data transfer will impede the rapid delivery of (digital) services. To relieve a part of this burden for organisations, it is advisable to explore whether consistency between Member States regarding powers and safeguards in the area of intelligence and security services could provide a solution. It cannot and should not be expected from organisations that they should assess and evaluate this framework.

Also, it must be recalled that the right to data protection is not an absolute right but should instead be balanced with other rights, such as freedom of trade, of expression and of information. Therefore, the Recommendations should

[1] European Court of Justice (ECJ) judgement in case C-311/18, *Schrems II*, paras. 121, 134, 146.
[2] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 42.
[3] ECJ judgement in case C-311/18, *Schrems II*, paras. 112, 121, 126, 146 and 203.3.
[4] See Standard Contractual Clauses for the transfer of personal data to third countries, clause 2 and 3.

not impose disproportionate measures and should rather enable data exporters and importers to balance the different (fundamental) rights and interests at stake.

Moreover, the requirement to apply extensive encryption to all stages of the data processing, making third-country authorities' access impossible or ineffective, would result in organisations having to implement expensive encryption methods, even in cases where the risk is (very) low. The implementation of such technical measures is difficult and costly. This would be disproportionate, and particularly burdensome for SMEs. The level of protection should equate the level of risk. In addition, disabling access to the data in third countries can only serve as a potential measure to protect personal data in transition and 'at rest'. It is not a workable measure for services that must access communications or related personal data to deliver these services (e.g. communication services such as e-mail and videoconferencing, or money transfers). For many online services to work accordingly, it must be possible to process the information unencrypted. The Recommendations should ensure that the proposed technical measures are workable in practice, and it should be left to data exporters to determine whether a particular measure adequately protects the transferred data.

Furthermore, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider 'all actors participating in the transfer'. This would mean that the data exporter, assisted by the data importer, would be required to list the full chain of sub-processors. This obligation is detached from the digital world of today. In complex supply chains and different cloud structures with multiple parties (which, in software-solutions, are the current standard), this obligation is simply not feasible.

### 3. The Recommendations should clarify that contractual measures may provide sufficient safeguards

The draft Recommendations suggest that contractual or organisational measures on their own cannot provide the required level of data protection and that technical measures are, in some cases, the only measures that may enable personal data to be transferred. This reading of Schrems II is too restrictive. It also contradicts the fact that the GDPR is intended to be 'technology neutral', and therefore should not impose any technical or technological requirements. As long as the data importer does not disclose data to third-country authorities, or it notifies the data exporter accordingly, the parties may rely on the Standard Contractual Clauses. Under this reading, in some circumstances, contractual measures alone can provide the additional safeguards needed to safely transfer data to a third country.[5] An obligation to challenge a third-country authorities' request, as well as transparency obligations to inform the controller of such a request, is important in determining if an interference will effectively take place. This is tied to our point above about the need for a proportionate response.

Organisational measures such as codes of conduct and certification mechanisms are appropriate safeguards under the GDPR and can adequately assist organisations in assessing and complying with relevant regulation. It should be left to data exporters and importers to evaluate which measures are appropriate in the specific context and 'in the light of all the circumstances of that transfer'.

[5] ECJ judgement in case C-311/18, *Schrems II*, paras. 132-139.

## 4. The Recommendations should clarify how they should be applied in relation to Binding Corporate Rules

Paragraph 58 to 60 of the draft Recommendations are unclear as to the impacts of the draft Recommendations on Binding Corporate Rules (BCRs). More precisely, it is not clear how the draft Recommendations should be applied in relation to BCRs and to what extent additional supplementary measures are required. In this respect, it should be noted that BCRs already require extensive work from organisations and are approved by European data protection authorities. They should, as such, be considered as sufficient and satisfactory contractual commitments enabling the transfer of personal data outside of the E.E.A.

## 5. The Recommendations should make clear that enforcement by DPAs will be appropriate

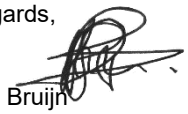
The Schrems II judgement has a wide-ranging impact on EU organisations, and complying with the judgement and the accompanying Recommendations requires major efforts. The EDPB has emphasized that DPAs will be responsible for enforcing the Recommendations. This leads to a challenging position for DPAs. The draft Recommendations accentuate that DPAs could impose 'corrective measure[s] (e.g. a fine)' if they determine that a data transfer does not comply with the Recommendations.[6] Here, DPAs should be wary of inconsistent or even exemplary enforcement.[7] It is recommended that the Recommendations advise DPAs to work together with data exporters to find workable safeguards and allow organisations to implement these solutions.

It is also unclear how EU DPAs will have the capacity to assist organisations in their assessments of all applicable local law (see remark nr. 2), given the nature of national security law and that each law will have to be put into the context of the risk that jurisdiction faces.

Furthermore, enforcement measures should also reflect and take into account the wider public policy, economic and/or social impacts it might have. Restrictions on data flows will ripple across all aspects of our society and should not be taken in isolation without a comprehensive review of the total impact. This assessment could also include coordination with other regulators and governments.

We would like to thank you again for giving the opportunity to provide feedback. Should you have any questions, please do not hesitate to contact us.

Kind regards,



Lotte de Bruijn
Managing Director NLdigital

[6] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 54.
[7] These risks are not taken away by the possibility for DPAs to refer to the EDPB for an opinion if they consider that transfers of data to a third country must, in general, be prohibited, as mentioned in ECJ judgement case C-311/18, *Schrems II*, paragraph 147.