LERU concerns re "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

Feedback 1

- The most difficult aspect of the new requirements is that there is an expectation that organizations should / will have an in-depth knowledge of every non-EEA countries laws which could affect directly / in directly data protection legislation. This is unrealistic and will lead to mistakes being made through simple lack of knowledge / understanding.

- The new requirements will cause delays in what is a fast paced and demanding area of our business. Whilst I started preparing documentation/templates in July to respond to the original judgement, the new process will not be seamless, will require information that has previously not been requested and will require discussion/agreements between all affected parties which will not be simple where parties are numerous in number and span several countries both inside and outside the EEA and we have zero clarity of how this will work in practice.

- Relevant is the fact that during the same week they released guidance re current SCC's they also released the new SCC Drafts meaning we will be demanding a lot of changes in the immediate future whilst knowing that in a yet undeclared period of times (lets say 3-6 months) we are going to have to do it all again as the old SCC will likely be deemed null and void meaning the new SCC's will need to be signed causing further disruption.

Feedback 2

- Whereas the CJEU (paragraphs 132 to 135 Sentence C-311/18) established that the data controller shall take appropriate supplementary measures to guarantee an essentially equivalent level of protection under EU law, and whereas the GDPR o the Court do not define or specify the "supplementary measures" or "additional safeguards", the guarantees implemented in research projects according to Article 89.1 GDPR (for example, pseudonymisation) shall be considered sufficient to comply with the CJEU's requirement, that is, to guarantee an essentially equivalent level of protection under EU law.

  Consequently, if the data controller adopts the standard data protection clauses and the guarantees in Article 89.1 GDPR, the adoption of supplementary measures to comply with the requirements established by the CJEU will be not necessary.

Feedback 3:

- Switzerland is not considered as a third country within these recommendations. On the basis of an EU-CH "Adequacy Decision", all EU-CH data transfers are considered as "intra-European".

Feedback 4:

We understand the concern by the recommendations made by the EDPB, on foot of the judgement of the CJEU C-311/18 (Schrems II) on 16 July 2020. We welcome the recommendations made by the EDPB, to address the implications of the Schrems II judgement, and in particular, the EDPB's attempt to define what could constitute 'supplementary measures. We have included our feedback with reference to the six steps highlighted in the Recommendations.

1. Know your Transfers

We initiated this exercise within Trinity, post Schrems II, and acknowledge that, in a university environment, this can be a very difficult exercise to complete, given the scale and complexity of the university structure, and the lack of resources for the completion of such a complex task. We have not completed this data mapping exercise at the time of writing this note.

2. Identify the Transfer Tool you are relying on

We would like to share our experience of the transfer tools that we rely on, so that we can open a dialogue as to which transfer tools might be preferable for research purposes.

- In situations in which adequacy decisions have been adopted, we understand that we do not need to take any further steps (other than to monitor such decisions.)
- We have relied upon explicit consent as a derogation under Article 49 for once off or occasional transfers for research purposes. In particular, for U.S transfers, as we have found that U.S research institutes are often not permitted to accept foreign jurisdiction (which has ruled out adoption of SCCs).
- We do not envisage any difficulty putting SCCs in place outside EEA with supplemental measures that are standard practice in research, as outlined in case study 2 of the Recommendations (paragraph 80).

We would be interested to understand whether any of our LERU counterparts, have been successful in negotiating SCCs with U.S research institutes?

We would propose that explicit consent is an acceptable mechanism for any future transfers outside EEA for research purposes.

We fully recognise that gaining explicit consent is not a straightforward process and may not be possible in all situations (particularly if the data was collected several years ago.)

We would welcome further guidance on the extract below, which is taken from a separate Opinion of the EDPB on the use of derogations under Article 49.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

The information provided to data subjects in order to obtain consent for the transfer of their personal data to third parties established in third countries should also specify all data recipients or categories of recipients, all countries to which the personal data are being transferred to, that the consent is the lawful ground for the transfer, and that the third country to which the data will be transferred does not provide for an adequate level of data protection based on a European Commission decision.

In addition, as mentioned above, information has to be given as to the ***possible risks for the data subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards*** *"Such notice, which could be standardized, should include for example*

information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country."

Can we request that the EDPB provide appropriate text for such standardised notices, for transfers to the US in light of Schrems II.

3. Steps 3 – 6 only apply if there is no adequacy decision nor an Article 49 derogation, and if the **assessments reveal that the third country infringes the transfer tool.** We envisage very limited scenarios in which this would apply to our collaborations.

However, looking to the US context, and given that our 'specific' context is research, we believe that the surveillance type legislation (S. 702, FISA) which was the primary cause of concern in the Schrems II case. only applies to electronic communication service providers, and as such the implications of Schrems II, are not as severe as they may appear at first glance for Universities transferring data to other academic institutes for research purposes. We would appreciate confirmation of this view by the EDPB and we would welcome an open dialogue on this point with our colleagues in LERU.

Additionally, we note that the supplemental measures cited within the recommendations are already used as standard by researchers:

- research data is almost always shared in pseudonymised format, with the key held in EEA. Indeed, the data is often stripped of any identifiers, to the point of being 'anonymous' in the hands of the recipient;
- the exercise of data subject rights, as outlined in paragraph 34, should not be problematic, as we would be the contact point for such requests;
- binding contracts are put in place for any transfer of data (even if anonymous). For any transfers of pseudonymised data, these contracts stipulate how to deal with withdrawal of consent (if this is the tool which we rely on for the transfer itself.)

<u>Further clarification required</u>

1. How do we as individual controllers assess whether a particular third country has laws which are necessary and proportionate? Whilst we welcome the guidance provided by the EPDB on this matter, we believe that it is the Commission's role to carry out such investigations and to advise SAs , who in turn advise Controllers.
2. How do we verify the rights of redress that individuals have, if their data is accessed by public authorities? More guidance is required from the EDPB or the Commission. This relates back to point 1, and to point 5 below. We need centralised review of countries outside EEA and their legal systems.
3. Is there any approved code of conduct which could be established for researchers pursuant to (2 (e) of Article 46? If LERU were to establish one, could this be an alternative tool for transfer? It would still be subject to supplemental measures, but it might be an appropriate alternative to explicit consent?
4. Does FISA apply to research institutes or is there any other surveillance type operations which might apply outside of EEA? Surveillance laws in France, Belgium and the UK have also been found to infringe GDPR. How can these transfers be considered adequate where those outside EEA are not?

5. We would welcome the EDPB providing appropriate text for standardised notices, if we are to continue to use explicit consent as the most appropriate mechanism for transfers to the US (or elsewhere outside EEA) for research purposes.
6. If an individual gives consent to sharing outside EEA with academic institutes (no controllers named), and is put on notice that such sharing may not offer an equivalent level of protection to the GDPR - is this sufficient or would we need to reconsent prior to each transfer in order to be specific about the particular controller? How does this impact on any transfers on from that third party?

Feedback 5:

Request for guidelines for the use of the derogation in Article 49, paragraph 1, letter d): "The transfer is necessary for important reasons of public interest;"

Is it possible to use this derogation in research collaborations with partners in third countries provided a legal basis exists in national legislation as laid down in Article 49, paragraph 4?

Alain Smolders,
04/12/2020