Hello,

First of all I would like to thank you for the great work you have done so far!

I went through the guidelines many times now and yet I didn't find anywhere mentioning how we can tackle countries that have surveillance laws with extraterritorial scope, such as FISA or Cloud Act.

I suppose we then have to apply supplementary measures, especially technical ones (encryption). But it would be good to mention this case as well and provide more guidelines on that matter, because 99% of businesses today in the EU are using US providers that fall under the extraterritorial scope of US surveillance laws.

Although it may look self-evident that supplementary measures should apply in this case as well, many controllers, in order to avoid the extra hussle, think like that:

-I am using for example AWS and I choose AWS Region Stockholm. Therefore, no data transfer occurs, so first, I don't need a transfer tool and second I don't need any supplementary measures since data is not leaving the EEA.

This is in contrast with the Schrems II and when I am consulting my clients to apply supplementary measures, they ignore me because even at step 1 (know your transfers) of the 6 step assessment that EDPB recommends, it appears that the data stays in the EEA and they choose to stop there.

I have discussed it with many fellow data protection consultants and we all agree that supplementary measures should be applied in this case as well. But maybe it is just our opinion and we are wrong, so it would be great to address this issue.

What I advise my clients to do is, during the data mapping, map out all the processors or joint/independent controllers with which they share personal data with and then do something like a "background check" if they are subject to any surveillance law with extraterritorial scope. So that they are aware of that from the very beginning that there is a risk there. Because the step 1 that you recommend (map the transfers) will not show any risk in this specific case.

I hope that you take under consideration my concerns and address the issue that is of high interest among data protection professionals.

Feel free to contact me if you have any questions or if you need more clarifications.

Best regards,
Elisavet Dravalou