ANONOS

Schrems II Lawful Cloud Processing

Additional Safeguards DO EXIST
A Defensible Business Position IS ACHIEVABLE

SPEAKERS


Gabriela Zanfir


Patrick Van Eecke


John Bowman


Mark Webber


Magali Feys

FUTURE OF PRIVACY FORUM | Cooley | PROMONTORY an IBM Company | fieldfisher

Presented by: ANONOS

Webinar Summary

Over 59 countries participated in the 29 October 2020 Schrems II Lawful Cloud Processing webinar; 1700 companies and firms were represented; 41% were General Counsels or report to the General Counsel; 35% were privacy professionals - Chief Privacy Officers and Data Protection Officers; 22% were Outside Legal Counsel and Advisors; and 2% were Government Officials.

These numbers and seniority of participants emphasize how important it is to gain greater clarity as to the availability and applicability of Additional Safeguards. The goal of the webinar was to provide clarity on how companies can continue business operations without concern over termination of data transfers under Schrems II.

Webinar Panel Discussion

(covering the top 5 audience FAQs)

FAQ #1

Panel Discussion Summary:
Schrems II is a Board/CEO-Level Issue

The panelists discussed reasons why waiting for further clarification before establishing a defensible position for ongoing use of US-based Cloud, SaaS and outsourcing solutions involves considerable risk and should be raised to the Board/CEO. Reasons included increasing potential personal liability for Board Members/CEOs, and obligations of auditors to report data protection violations to authorities under International Ethics Standards Board for Accountants (IESBA) Non-compliance with Laws and Regulations (NOCLAR),

Post Webinar Update: The importance of briefing your Board of Directors/CEO and creating a defensible position for ongoing use of US-based Cloud, SaaS and outsourcing solutions was highlighted by two separate announcements made on the same day as the webinar:

- The NOYB was approved to pursue collective action on behalf of data subjects directly against data controllers and processors without having to go through the GDPR "one-stop-shop mechanism" for Data Protection Authorities.
- The European Data Protection Supervisor (EDPS) instructed European Union Institutions to:
    i. Avoid new processing activities involving transfers of personal data to the United States (which includes US-owned Cloud and SaaS providers, regardless of where servers are located);
    ii. Complete Transfer Impact Assessments (TIAs) for all data transfers; and
    iii. Expect joint EDPS/EDPB guidance, compliance audits and enforcement actions for transfers towards the U.S. or other third countries on a case-by-case basis.

FAQ No. 1 Excerpted Panelist Quotes:

Mark Webber (fieldfisher): I think it is an issue that should be discussed at all levels within an organisation…I think it's really heartening to see that's the beginning of the feedback that we're seeing because we're all looking for a defensible position.

Patrick Van Eecke (Cooley): Well, I see exactly the same kind of evolution where I'm receiving client calls exactly on that topic. Do I need to make the Board aware? Do I need to make the Stockholders aware of these things? And yes, you have to, I believe, because when you're looking at risk exposure and this is what it is about, you always have to have that kind of calculation on the one hand the fine multiplied by the probability of "Is this going to happen?" …So, if you are an auditor or if you have the responsibility within an organisation to calculate the probability of a sanction for an illegal data transfer (Yes, the fine. That's clear.), now the probability from zero should probably be increased dramatically because of the fact that it's now so much in the news…the Director's liability in Europe is a hot topic and this kind of personal liability we see for GDPR infringements are similar to Director's liability, for example, for environmental infringements. And here, of course, today, it's going to be very, very difficult for a Director of a company to say: (1) "I didn't know about it." Because you do know where the data are being transferred to. (2) "I didn't know that it was illegal." Because it's all over the newspapers. (3) "I didn't know we had to do something." This is not going to fly and that's also what Mark said, but we don't know yet what we have to do. It's not clear yet, but we know that we need to do something and that is of course something that we have to discuss here also during the webinar. What can we do to exactly have this kind of acceptable business kind of position?

Gabriela Zanfir-Fortuna (Future of Privacy Forum): I would say when I saw the question, I thought: "Oh my! That's the easiest question that one can ask around Schrems II because it has an absolutely immediate answer." And that answer is an emphatic "yes". Yes, you should bring this to the attention of the Board because it's very relevant and you've heard Anna Buchta two weeks ago in the webinar saying that DPAs and Supervisors are looking at this as meaning a moment in time where things will start being different than they were before. And I would agree with this point, Gary, that these orders that DPAs can take can actually affect much more a company or a business than a fine…you also have the risk of actually not being fined but being on the receiving end of an order to erase data or to stop transfers. This is one of the super big innovations of the GDPR compared to the former directive. The fact that Data Protection Authorities now have increased powers that includes this type of orders. And of course, there is an internal process and I agree with Mark and with Patrick to this extent that

you need to pay attention to what you report to the highest level in your company, but this is a matter that they should be aware of for sure.

Magali Feys (Anonos): Well, first the short answer. Do the board of directors and need to be made aware? Of course, yes. Now, the longer answer. It's not that I disagree with Patrick or Mark. Not at all, but I think it's really what Gabriela said. Schrems II is, I think, unique because it obligates the Data Protection Authorities to stop unlawful data transfers rather than to impose penalties. And so, I think that the potential impact of terminated data flows can be naturally much more adverse to the operations of a company than fines. And we have already seen some Data Protection Authorities coming back with their opinions and asking to stop certain international data transfers whether it was with regard to medical or health data, whether it was with regard to the learning platforms that are used now in COVID times for the children that have to stay at home.

John Bowman (Promontory): Most international organisations will consider themselves to be data-driven organisations. Data does flow from entity to entity and from country to country. And if the appropriate safeguards are not in place, either through the normal controller processor arrangements or through the international data transfer mechanisms, then they will be in violation of the GDPR…I think the point that Gabriela made, in particular, about the ability of regulators to suspend data flows or terminate them is a very powerful one and if those safeguards aren't in place then it could be a sanction that they could enforce running alongside the administrative sanction regime now of course that individuals do have the right to judicial remedies as well. So, if they feel that there has been a violation, they don't necessarily have to go through the regulator routes. They could take it to the courts and see what happens there. And on top of that, certainly in the UK at least as I can't speak for other European countries, but there is Director liability related to criminal offenses, which can be committed under the UK Data Protection Act. So, Directors, Secretaries of companies, and offices of the companies can be held liable in the context of a criminal offense committed under the data protection legislation and that could include various things including the re-identification of de-identified information, without authorisation. That is a criminal offense. So, Directors certainly do need to be aware of that.

FAQ # 2

Panel Discussion Summary:

No, you cannot rely solely on statements by US Cloud/SaaS/Outsourcing providers that their SCCs enable lawful data transfer.

Data controllers have an affirmative obligation to ensure that SCCs are augmented with “supplementary measures” that ensure protection equivalent to EU data protection laws. This obligation remains the sole obligation of a data controller under Schrems II unless it is expressly assumed by a cloud provider, in which case it becomes a shared responsibility of the parties.

FAQ No. 2 Excerpted Panelist Quotes:

John Bowman (Promontory): Yeah. Well, I think the Schrems II ruling had some quite specific advice in terms of the obligations of the data exporter. So, this would be generally an EU data controller and the recipient organisation wherever they may be. So, the key thing that needs to be taken into account effectively are appropriate safeguards in place…I think really the whole ecosystem needs to be bought into this whether it’s the data exporter, the providers, the services providers, the vendors, the controllers, and the processors and sort of understand that ultimately the objective is to safeguard the data and effectively provide the actionable rights, which the court demands in the third country that the data are transferred to.

Gabriela Zanfir-Fortuna (Future of Privacy Forum): The question of what is a transfer and what falls under this ruling as well as under Chapter 5 of the GDPR is a question that I’ve been spending a lot of time thinking about and I think I would frame it a bit differently, Gary. It’s not necessarily an issue about who owns the business that has the server that’s located in Europe. Because from my point of view, that’s not really the criterion here. The criterion is whether there is any access to that server from outside of Europe. There are a lot of interpretations that push towards an answer to say: “No, that’s not a transfer.” And I heard my friend, Romain, also kind of saying the same theme. But based on my experience working on this for some years now and also based on something that the EDPB actually included in question 11 in their FAQ, the reality is that access from a third country constitutes a transfer of personal data. So, access from outside the European Union to data that is in the European Union constitutes access. And you know, there are many theoretical arguments that go to support that. But the easiest reference that I can make to give credibility to this

interpretation is as I was mentioning an answer from question 11 in the EDPB FAQ because access would mean transfer as well.

Now to the question of how much someone can rely on statements by the big cloud providers, I would prefer not to comment on that because obviously we might don't have access to all of the information that would be needed to provide an answer. But I would point out to controllers that are relying on cloud providers as processors that they should have entered into an Article 28 agreement with them - that's a controller processor agreement - and one of the clauses in the Article 28 agreement must have referred to audits and inspections because that's a requirement under the GDPR. And if you have a proper Article 28 agreement in place with them even if it was a template agreement, you do have that audit provision, which has obviously different shapes and forms. It can be a paper audit. It can be an audit that can be performed just once per year or I don't know how that was shaped into those agreements, but you do have mechanisms to actually check and see whether what they claim is true.

Magali Feys (Anonos): Well, yes, I do believe that the mere access as Gabriela pointed out I think was also indeed underlined by the EDPB that mere access is indeed a transfer of data or constitutes what is understood as a transfer of data under the GDPR. It's not to blame those cloud providers because I don't think that is what is the question is really about, but it is just to point out that of course by actually doing or providing some sort of services that even regardless of the location of the server being in Europe, that you are still actually falling under international transfer of data considered under the GDPR. And so, you fall under the Schrems decision. So, I think that is very important to take that into consideration.

And then, are the SCCs indeed enough? No, I think that is exactly the ruling of Schrems II where they said SCCs are valid. But next to that, you have to do it and that's what was already touched upon in the other webinar is what some called data transfer impact assessment and you really have to see who has access or to whom you are transferring the data and see whether that country has an equivalent set of rules if it doesn't have an adequacy finding and adequate set of rules in order to protect the rights of the data subjects. For example, it could be in some countries or with some data transfers SCCs could be enough because I don't think Schrems II ruled that out but it's stated and definitely with regard to the US that with the surveillance laws, they were definitely not enough.

Mark Webber (fieldfisher): SCCs aren't enough on their own, and there is joint responsibility and we knew that without Schrems II there is an obligation around transfers, which is either imposed contractually via Article 28, which the other panelists have talked well about or it sits there in the GDPR processors have to comply in respect of law transfers as well…I think

what we are talking about here is layers of protection, and I suspect we will come on to talk about this when we talk about Pseudonymisation and encryption and other safeguards...I'm definitely an advocate of using as many safeguards as possible and layering them up and I think a number of us have talked to that already…Right now, I think some of the problem is someone out there just wants to run and put some kind of standard contractual clause in place and say "I've done it. Look I have a tick in the box." Anyone who has ticked the box today and thinks they have closed off their transfer issue is wrong…The cloud providers are taking this incredibly seriously because to Gabriela's and I think to Maggie's point, this gives competitive advantage. If you can show that you're on top of this and you have new techniques to offer and that you're reacting and you're able to articulate what Schrems II means and help your customers, you're going to be in a better position.

FAQ # 3

Panel Discussion Summary:

Yes, BCRs and SCCs are both covered by Schrems II.

The Schrems II FAQs published by the EDPB make it clear that "...the Court's assessment applies as well in the context of BCRs…" and "supplementary measures along with BCRs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee."

FAQ No. 3 Excerpted Panelist Quotes:

Patrick Van Eecke (Cooley): BCRs, are they affected by Schrems II just like standard contractual clauses? And yes, they are. That's very clear. Gary, you just mentioned that as well. So, the European Data Protection Board even stated explicitly that you also need to look into BCRs in order to make sure that you can have an appropriate data transfer. Yes, they are impacted but it doesn't mean they are invalidated and that is a very important point I want to make. I even believe that BCRs for certain circumstances namely intra-company data transfers that they are the solution to the issue…Other organisations that are currently looking to find a solution for this whole kind of debacle, I would say I would highly recommend to look into the opportunity of BCRs because many other companies are doing it. It's a lot about what others are doing. It's a lot about peer pressure. It's a lot about, as mentioned I think by Mark, getting competitive advantage. BCRs is one of those things, which certainly also adds to your competitive advantage as a company. But again, it's just for intra-company data transfers.

FAQ #4

Panel Discussion Summary:

Yes, properly performed Data Protection By Design and by Default processing – including HR data – can be processed via Pseudonymisation as an Additional Safeguard.

Unlike many other use cases, consent-based processing will rarely be an option for employee-related data. This is because of the imbalance of power between employers and employees; employees can only freely give consent in exceptional circumstances. It is extremely difficult for employers to rely on the lawful basis of consent to process employees' personal data.

With consent generally not available, attention naturally turns to contract-based processing. However, in that case processing is limited to what is strictly necessary for the performance of the contract. In the employment context, this might cover payroll and benefits administration, but cannot extend to secondary uses like Talent Analytics. Moreover, the use of contract does not constitute an additional safeguard that would enable international transfer of this data for processing outside the EU for the same reasons SCCs alone are now inadequate - government agencies that might surveil the data are not bound by the contract.

As discussed in the first Schrems OO webinar, one of the consequences of the Data Protection by Design and by Default (DPbDD) obligations under Article 25 of the GDPR is that if processing can be done using de-identified data it must be. Note that this is true whether processing is done within the EU (localised), or outside the EU. Using GDPR pseudonymisation to de-identify data can be quite useful in establishing the grounds for processing based on legitimate interests.

FAQ No. 4 Excerpted Panelist Quotes:

Mark Webber (fieldfisher): Yeah. I can say very briefly I think employee data is personal data. Personal data is regulated by the GDPR. So, you are applying very similar positions. I think when we get too focused on data transfers, we can forget that the GDPR puts in a number of other obligations and whatever you're doing as a controller with data, you need to be processing it fairly and lawfully. So, you need to be establishing the grounds for processing that employee data in the first place. And there are challenges with consent. You are more likely to be looking at legitimate interest processing or contractual necessity for these limited resources and even statutory obligation for certain types of reporting. So, you need to establish that.

Then, you need to look at the transfer and how you are doing the transfer. Employee data can be transferred subject to BCRs and subject to the SCCs, but you're looking at the same kind of things. You are doing a transfer impact assessment…You need to also work out whether it's actually necessary. There's a lot of general replication of databases I find when actually not all that data needs to move in the first place. But yeah, context is king and there is more to deal with. Patrick's and others in Europe will be well aware of work councils and other approvals that might be needed, and you need to be thinking about other kinds of sanctions and permissions that you get from workers generally.

John Bowman (Promontory): I agree with everything that Mark said. Although there might be some outsourcing maybe to business process outsources for administrative purposes like pensions management and so on. But as Mark said, context is king. As a data controller, you should always understand what your data flows are and what agreements and arrangements that you have in place to transfer the data and what the recipient regime is like. As Mark did suggest, certainly for EU-based controllers, the handling of employee data often has its own sort of specific requirements, works councils, for example. In more so, the sensitive industries maybe financial services, which may be vulnerable to fraud, or those kinds of industries where there might be measures in place where you know there is sort of a data leak prevention…The employers really have to understand their legal bases in which they are able to undertake those particular activities. Now, if things like fraud prevention or some kind of potential crime prevention monitoring is taking place and that information is transferred outside of the jurisdiction, then I think there is a high degree of sensitivity around that type of information. And of course, maybe you'd have to make some sort of assessment that if there is a recipient in another country, whether national authorities may well take some sort of interest in some of that information as well. So, that's when you start to think about your supplementary measures and appropriate safeguards. So, I think just to conclude, employee data processing brings its own challenges and its own requirements and own considerations, and they should be considered in around both in terms of the controller processing and any information, which is transferred to third party or even to another entity of the same organization that is located in a third country.

Magali Feys (Anonos): Yes. So, first I want to start with the bold statements that I believe that with Schrems II the writing was on the wall. And so, there was nothing really surprising. And as Gary already touched upon, people or companies that already implemented Data Protection by Design and by Default have a better job because I think with regard to international data transfer, that is exactly. It's a little bit too bold and maybe too short but it's what we really have to start thinking or we had already thought about the fact that also with relation to international data transfer

that Data Protection by Design and by Default should be embedded in the way we thought about that. And so, I believe that essentially, any EU employee related data processing that can be done in a multi-step Data Protection by Design and by Default manner can be completed using Schrems II compliant Pseudonymisation.

Gabriela Zanfir-Fortuna (Future of Privacy Forum): Well, obviously, transfers of employee data are covered by Chapter 5 of the GDPR. But good luck there, I would say. The fortuitous thing with these transfers is that you do have a direct relationship with your employees and I would say it's much easier to argue that your transfers are not massive even though they might be repetitive, so you are in a better position to use one of the derogations under Article 49 for sure. And then, of course, to the extent you can bring additional safeguards to that, the processing and the transfer lawfulness would be certainly supported if you want to go the route of relying on one of the derogations. I think the other panelists have already covered the option to rely on SCCs and on BCRs for that purpose.

FAQ # 5

Panel Discussion Summary:

No, the GDPR heightened standard for Pseudonymisation is not the same as the "casual" understanding of the technique.

The requirements necessary to satisfy the GDPR definition of Pseudonymisation are very different from the pre-GDPR "casual" understanding of the term – you must now satisfy dramatically heightened requirements. Only a very small subset of what might previously have been considered “pseudonymised” data would satisfy the new definitional standards under Article 4(5). The new definition now requires that:

- The processing of personal data must be accomplished in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information;
- Such additional information must be kept separately; and
- Technical and organisational measures must ensure that the personal data cannot be attributed to identifiable persons without requiring access to the separately and securely stored “additional information.”

It is critical to note that the new heightened level of Pseudonymisation under the GDPR is, as a consequence of the breadth of scope of personal data, now defined as an outcome for a dataset and not just a technique applied to individual fields.

By elevating Pseudonymisation to an outcome, GDPR-compliant Pseudonymisation requires protection of not only direct identifiers but also indirect identifiers, and potentially attribute fields as well. In addition, instead of being applied only to individual fields, GDPR-defined Pseudonymisation, in combination with the GDPR definition for Personal Data, now requires that the outcome must apply to a data set as a whole (the entire collection of direct identifiers, indirect identifiers and other attributes). This means that consideration must be given to the degree of protection applied to all attributes in a data set. Finally, the foregoing must be accomplished while still preserving the data’s utility for its intended use, which under Schrems II would include international data transfer.

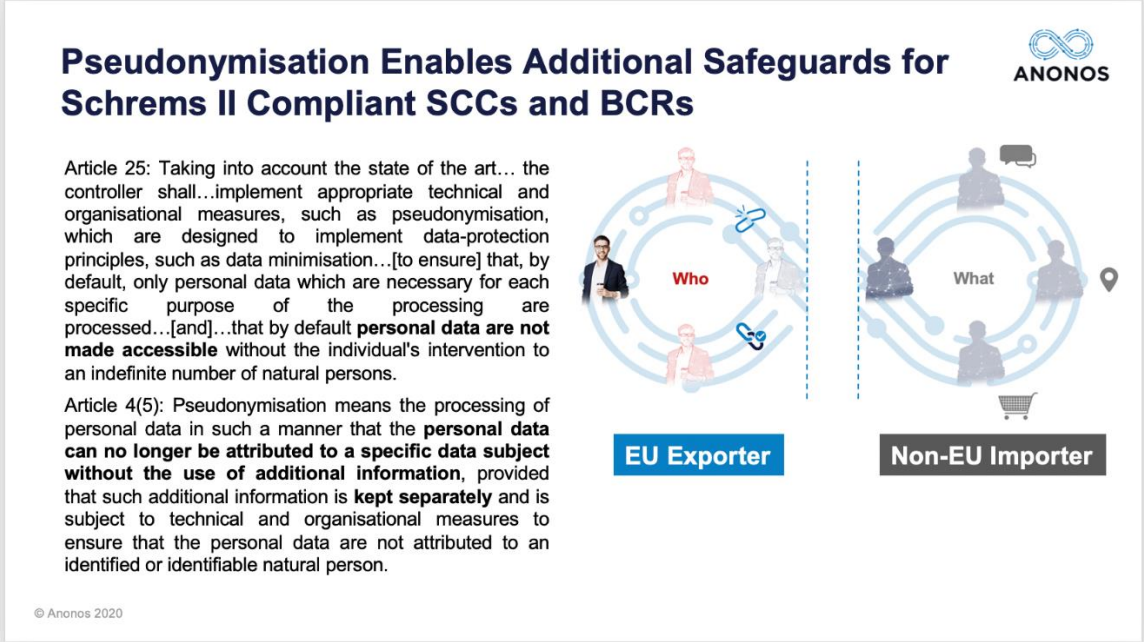
As a result, pre-GDPR “casual” approaches (using a static token on a direct identifier, which unfortunately is still widely and incorrectly referred to as “pseudonymisation”) will rarely, if ever, meet the heightened GDPR requirements of Pseudonymisation.4 This also means that old or “casual” approaches fail to achieve the new statutory requirements for the term and therefore will not satisfy the requirements for supplementary measures to enable lawful international data transfers under Schrems II.

FAQ No. 4 Excerpted Panelist Quotes:

Magali Feys (Anonos): The GDPR has now given a new and higher standard to Pseudonymisation. I think it is very important for people to understand the concept and it's no longer a technique but really a concept under GDPR that it's not just failed anonymisation or taking away the direct identifiers but that it goes beyond that. And if you then take that heightened level of Pseudonymisation, then you will see why we take it as really a central element in the Data Embassy principles, which we submitted to the European Data Protection Board because as an outcome, it really enables data minimisation under Article 5 and it is the establishment and the enforcing of Data Protection by Design and by Default techniques, which restrict processing to a form of personal data that does not enable the identification of the data subjects and that once again also gives you the benefits under Article 11(2) and 12(2). Whether you keep that additional information for the relinking only in the EU, you also have lesser obligations with regard to the data subjects' rights because you already protected them by applying this Data Protection by Design and by Default concept. So, that's why we really believe and it's a key element of the Data Embassy principles but it is of course very important to then understand that we took the heightened new level of GDPR-compliant Pseudonymisation when you read those Data Embassy principles.

Mark Webber (fieldfisher): It may just be worth it for the audience to just take a step back because we were really talking about Schrems II and this focus on national security access to data. And of course, Schrems II was really decided on the fact that potentially national security government states might be getting access to that personal data and then denying the individuals and their underlying rights in respect to that data because either they don't know it's been accessed or they can't then access their right to deletion restriction, etc., etc. So, we're looking at methodologies within our Schrems II analysis to reduce or limit access to that data. And yeah, that's why we talk about minimisation and Data Protection by Design and by Default principles to minimize that access. Because essentially if we've got strong security, we are limiting that potential access. The stronger that security, the harder it is to get that access, and the more likely we can justify the transfer of that data outside of the European Economic Area. So, that's what we are looking to do.

Now, Maggie has really well-described Pseudonymisation is one of those security measures. It's a technique which effectively stops an individual being attributed to certain data. It also preserves use of that data because it is unique in its own special way. So, it maintains some of the characteristics of a personal data once it has been transferred.



Your diagram on screen right now shows it is no longer the Who and it's some of the What. So, it is a powerful technique and I agree there is an enhanced definition. In some ways, I think whether it's an enhanced definition or not, I'm not sure it matters too much because I think many really haven't come across Pseudonymisation. I mean, we could barely say it before the GDPR. It's a difficult word. So, I think many are looking at it afresh. It isn't part of a vernacular that many are starting to consider, but it is one of those additional safeguards, which can be applied alongside things like encryption and minimisation. I think this is where as a technical measure it's fantastic if you compliment that with contractual organisation and policy measures and it begins to perform a set and a suite of safeguards, which can adequately protect that data when it's transferred and then you're doing your own risk assessment to work out whether it is powerful enough in those circumstances and that's what we are really talking about here.

John Bowman (Promontory): Well, again, I do agree with colleagues here. It is a powerful measure which can be applied. It doesn't solve all your problems in one go, but I think certainly in the context of Schrems II, it can be applied as a measure alongside the contractual measures that you have in place and plus the risk assessments that you have done. So, any sort of transfer, which is potentially subject to Schrems II so anything out of the EU to a non-adequate third country should be taken in the context of the risk assessment and the measures both contractual and technical, which are applied…So, I think the GDPR does call out Pseudonymisation in various parts of the text and clearly sees it as a way of providing some sort of privacy-enhancing measure. So, I think that's my view on the topic generally.

Patrick Van Eecke (Cooley): Now, talking about Pseudonymisation in the Schrems II context, I don't think and I think everybody agrees that this is the one and only solution. I don't think it's going to be sufficient. I don't think it's always necessary. But for sure, it is a great instrument in many different scenarios. And even I would take it one step further and that is to challenge the European Commission on pseudonymous data and could it become anonymous data if the Pseudonymisation key stays in European territory and you then send or transfer that pseudonymous data to the United States. But actually, what you are doing is you are sending pseudonymous data without a key so surveillance authorities would never have access to the key on European territory.

So, that could mean we could qualify those data or the pseudonymous data on European territory and it could become anonymous data and even Chapter 5 of the GDPR on data transfers would not be applicable because it's only applicable to anonymous data, and this is a discussion. I do believe it's a discussion that should be taken, that should be done, that should be undertaken. It's a discussion between the distinction between contextual anonymisation and absolute anonymisation. And there, I do believe that the GDPR I'm explicitly referring now to Recital 26 of the GDPR, which is different than the former Data Protection Directive Recitals and the idea of what is anonymous data and what's personal data. I do believe that that Recital 26 about reasonably likely means to be used to identify an individual using objective factors, such as costs and time needed, that kind of formulation should go into the discussion whether or not pseudonymous data being sent to the United States or any other country without sharing the key could actually be considered as anonymous data. It could be a solution for the Schrems II issue because, as Mark already mentioned, at the end it all boils down to are you able to prevent foreign surveillance authorities to have access to personal data in clear and that actually would be prevented.

Gabriela Zanfir-Fortuna (Future of Privacy Forum): The GDPR introduced Pseudonymisation specifically as a measure that decreases the risk of personal data processing with regard to data subjects. So, very clearly, pseudonymised personal data is personal data still. The GDPR indeed still applies to that data, which means that the transfers rules apply to that data as well. But there is also a recital in the GDPR Recital 28 that really spells out what the purpose of Pseudonymisation is, and that is the fact that the application of Pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. So, it's definitely a measure that supports compliance, decreases risks to the rights of the data subjects, absolutely a measure that should be taken into account.