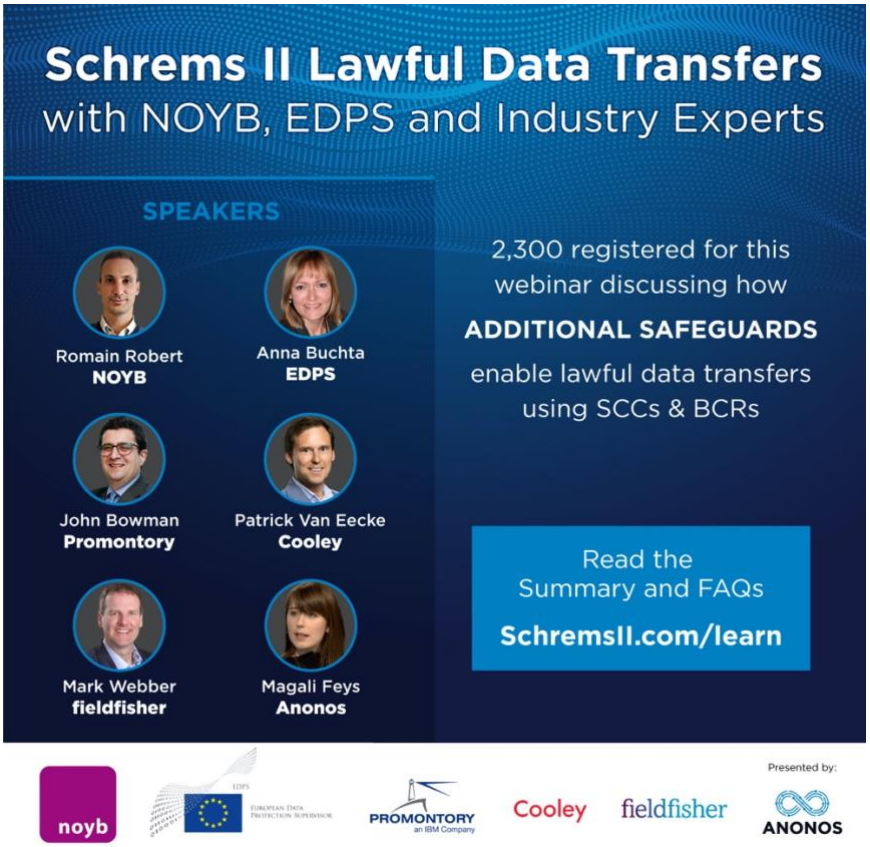
Schrems II - Lawful Data Transfer Webinar

Summary

Part I below are the top 25 Frequently Asked Questions (FAQS) from the 900+ questions submitted by the audience before and during the 8th October webinar, answers to be published in the **Schrems II - Lawful Data Transfer LinkedIn group.**

Part II below includes summaries of responses by the panelists to the four questions asked live during the **Schrems II - Lawful Data Transfer Webinar**; these answers are further qualified by the full transcript and video recording of the webinar at: **Webinar Transcript & Replay**.



One issue that all panelists unanimously agreed upon, as did 94% of the webinar registrants, was that a two-step privacy-respectful Data Protection by Design and by Default approach is required for all processing whenever possible. This includes, but is not limited to, international data transfers following the CJEU decision in Schrems II.

The Schrems II decision effectively imposed “precision” on general obligations under the GDPR. The decision now prescribes that EU data can no longer be lawfully processed in US-operated (or any other non-EU operated) clouds, SaaS or outsourcing services without “additional safeguards” that prevent the data from being subject to surveillance by the US (or other non-EU countries).

Previously, some companies engaged in “regulatory arbitrage” by choosing not to comply with privacy laws, by baking the cost of non-compliance into their cost of doing business. Of great significance is the fact that the CJEU ruled that such unlawful data transfers and processing must be *stopped*, rather than fined. This makes a “regulatory arbitrage” approach impracticable – lack of access to data halts business operations, and cannot be merely calculated into the cost of doing business.

The following information can assist with moving forward without regulatory arbitrage, so that lawful global data transfers can continue in compliance with the Schrems II ruling.

Part I: FAQs from Audience

Below are the top 25 Frequently Asked Questions (FAQS) from 900+ questions submitted by the audience before and during the webinar, answers to which will be published - one per day - in the Schrems II - Lawful Data Transfer LinkedIn group.

1. Are BCRs similarly affected by Schrems II like SCCs?

2. Board of Directors – should they be briefed on our Schrems II exposure? Stockholders? Financial auditors? Vertical industry regulators?

3. Can Additional Safeguards enable employee-related processing?

4. Can I rely on statements by US and other non-EEA/Equivalency Country cloud, SaaS and other service providers that their Standard Contractual Clauses (SCCs) enable lawful data transfer?

5. Can the "Next Steps for EU companies & FAQs" on NOYB website be used as Additional Safeguards?

6. Could Office 365 be modified to be legal knowing that data are sent outside Europe?

7. Differentiator of Anonos' solution in catering to the requirements of cross border data transfer.

8. Does Schrems II only apply to the US service providers and data transfers?

9. EDPB Schrems II FAQs require that EU data exporters ensure that data importers are not subject to laws that involve the indiscriminate and massive disclosure of data. How does data minimisation / Pseudonymisation satisfy that obligation?

10. Further details on Anna's statement that GDPR standard for pseudonymisation is not the same as the "casual" understanding - would like to hear more about the difference.

11. How are US-based cloud services providers such as Amazon, Microsoft, Google and IBM and their EU subsidiaries affected by Schrems II.

12. How can judicial redress be made available to EU residents with Additional Safeguards.

13. How does Schrems II apply to data residing on EU servers, but hosted by US companies?

14. How to properly set-up and use cloud-based SaaS clouds where most of the technical/organisational measures are on the side of the cloud service provider but the responsibility stays mainly with the customer, who quite often does not have the bargaining power to do anything.

15. If US and other non-EEA/Equivalency Country cloud, SaaS and other service providers fail to respond to risk assessment questionnaires about additional safeguards within three weeks, we recommend that the client suspend the data transfer since it is illegal. The standard contractual clauses (SCCs) alone are not enough, right?

16. Impact of Brexit following Schrems II.

17. Impact of Google Analytics and Facebook Cookie data transfers.

18. Impact of Schrems II on transfer of Clinical Trial Data and medical research.

19. Impact of US Department of Commerce White Paper.

20. Implications of the Cloud Act on Schrems II obligations.

21. Is GDPR-grade anonymisation technically possible?

22. More information of the Data Embassy Principles.

23. Please provide a Data Pseudonymisation 101 Overview for Big Data Analysis Risks.

24. Requirements for Additional Safeguards under Schrems II for SCCs/BCRs to Enable Lawful Transfer of EU Data to US and Other Non-EEA/Equivalency Countries?

25. What about some of the new privacy-preserving technology that is being developed -- synthetic data, differential privacy, etc.

Part II: Live Questions and Summary Answers

Q1

Panelist Question:

What processing situations create an obligation for data controllers to implement Data Protection by Design and by Default to enforce data protection principles like data minimisation? And is this limited to data transfer situations?

John Bowman (Promontory): Data Protection by Design and by Default applies to all data processing activities. It must be baked into any organisation's approach to designing applications and services, and ensuring that their data processing activities are safe, lawful, and transparent.

In terms of data transfers, there are measures which can be put in place to help provide technical and organisational safeguards to protect the personal data. The GDPR does give the examples of Pseudonymisation and encryption. But generally, the GDPR is technologically neutral: it's important to focus on the data processing principles, which can be supported by technological solutions. Those would be things like data minimisation, storage limitation, purpose limitation, and so on. That principle-based approach will help to safeguard data not only when it is in transmission and received, but most importantly when it is in use and at its most vulnerable.

Patrick Van Eecke (Cooley): I fully agree that Data Protection by Design and by Default are core principles of the GDPR and are always applicable. Of course, how you do it in practice vs in principle, is a different subject. I would go so far as to say that it's almost more of mindset than a process. Once you have a mindset of Data Protection by Design and Default embedded within your organisation, many issues will be resolved.

Mark Webber (fieldfisher): I think the core GDPR principles of Data Protection by Design and by Default apply whenever you're processing personal data. The definition of processing is very wide, and is applicable whether you're processing data for a small group in a single EU country or whether you're processing data for a large global organisation. But there are always elements of proportionality, and the GDPR is principle-based for a reason. It also requires us to look at what the state-of-the-art is: what's accessible at the time, and what's accessible to the organisation in question.

The appropriate technological and organisational measures necessary will depend on the circumstances.

Data Protection by Design and by Default also requires processing only the minimum data that is necessary. This could mean a combination of solutions and perhaps not processing the data at all. I like Patrick's idea of it being a mindset. But it's also about proportionality and risk. What kind of danger is there? What kind of things are we protecting? How can we protect it? There is an inherent tension when dealing with Data Protection by Design and by Default, as different people have different interpretations, different guidance, different circumstances, and different appetites for risk. We also must not forget that the burden of accountability sits with the controller. It is not a processor obligation.

Romain Robert (NOYB): I would agree that Data Protection by Design and by Default principles are universal. They are not only applicable to international data transfer, and there is no one specific situation when they should be applied. I also believe that Data Protection by Design and by Default is not only a nice *principle*, but that it is a “must have” that must be complied with. Data controllers must implement Data Protection by Design and by Default to remove all data that is not necessary for the desired processing or service.

It's also important to mention that Privacy by Design and by Default applies to all processing and not just to international data transfer. Nor will it make an illegal transfer legal. It could diminish or decrease the level of the fine, and may be taken into consideration by the DPA when determining the level of the fine. However, if a transfer is illegal, using a risk-based approach and Data Protection Privacy by Design and by Default are not your way out in these cases.

Magali Feys (Anonos): I agree with the idea that Data Protection by Design and by Default is a mindset. When advising companies, we see that while a lot of them have done the “GDPR exercise” at a policy analysis level, they have not embedded these policies into the technology or into their business systems. It is not a one-size fits all. The zero knowledge principle can work for certain companies, and not for others. You have to think about how you can define Data Protection by Design and by Default and embed it into your innovation. It's not only a principle to be implemented in the R&D Department, but it should also be embedded in the final business processes.

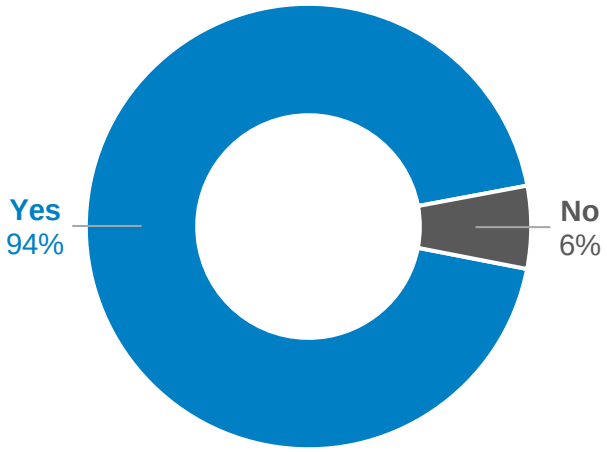
Anna Buchta (EDPS): I agree with practically everything that has been said. When we speak about the mindset of Data Protection by Design and by Default being baked in from the beginning, we should also ask ourselves the question: “Is the processing or the transfers really necessary? Can I do

what I need to do without processing or transferring the data to another jurisdiction?"

We should be careful not to fall into the trap of discussing how we can make sure that basically all the transfers that were taking place before Schrems II can continue after Schrems II. From the point of view of the regulators, given the fundamental constitutional importance of this ruling, there has to be a "before" and an "after" Schrems II. I would like to encourage people when they consider their processing operations to consider whether they are necessary and proportionate under the circumstances.

Audience Live Polling Question:

Do GDPR obligations of Data Protection by Design and by Default extend beyond international data transfers?



94% of the audience said "yes," that GDPR obligations of Data Protection by Design and by Default extend beyond international data transfers and 6% said "no," they do not extend beyond international data transfers.

Q2

Panelist Question:

What is your view of the legal principles that are set forth in the GDPR as they relate to these three different measures - encryption, anonymisation, and Pseudonymisation?

Anna Buchta (EDPS): Data which is anonymised in principle is no longer personal data within the meaning of the GDPR. So, that might seem like the silver bullet that solves all the problems. But there is considerable research that shows that true anonymisation in the age of big data, machine learning, and the capacity to quickly interconnect various data sources and databases is very difficult if not virtually impossible to achieve. I believe the Article 29 Working Party already expressed this warning in prior guidance on anonymisation. That was several years ago and the technical difficulties to truly anonymise data have only increased since that time.

Data that has undergone Pseudonymisation in the meaning of the GDPR remains personal data. However, the GDPR sets a certain threshold for the Pseudonymisation of data, which may not necessarily correspond to the typical understanding of this term - it is a heightened obligation that provides greater protection than what was associated with the term prior to the GDPR. This is often not understood.

Encryption will also not be the silver bullet solution. For data in transit and in storage encryption is an interesting solution. But it doesn't seem to be particularly useful if one wants to perform any kind of actual use or processing operation on the data.

Magali Feys (Anonos): It's all about a case by case analysis. One of the three could really suit your processing activity, or your business case. From a data security point of view, I think we have to be very careful about using only one technique. Secondly, encryption really protects data in rest and in transit, but from the moment you need your data, you have to decrypt it and you lose all safeguards at that time.

Anonymisation may still be possible, say for example with medical data. However, for potential secondary uses such as for retrospective research, you will need to access the original data which is not possible when using anonymisation. This is because you do not know today what data you may need tomorrow, and for which purposes. Some people believe the GDPR is limiting innovation. But the reality is that people who try to get out from under GDPR jurisdiction by applying anonymisation are limiting their own innovation.

I am a big believer in the heightened standard of Pseudonymisation as now required under the GDPR because it decouples identity from the information value of data to enable you to use a dataset that does not permit reidentification but allows for later controlled access to “additional information” held separately by the data controller for authorised uses. This requires protecting both direct identifiers as well as indirect identifiers across multiple and unknown data uses which requires advanced techniques like those specified by the EU Cybersecurity Agency, ENISA, as identified at www.EnisaGuidelines.com. With GDPR-compliant Pseudonymisation,, the original data can always be relinked for authorised processing which maximises innovation. People sometimes believe that failed anonymisation equals Pseudonymisation, but this is not the case under the GDPR. The new heightened version of Pseudonymisation recognised under the GDPR requires that it must be impossible to re-identify data subjects without access to “additional information” that is held separately by the data controller.

I think Pseudonymisation is the way forward and I think that’s why it was defined as an outcome under the GDPR and not merely as a privacy enhancing technique as it was prior to the GDPR.

Romain Robert (NOYB): I think security measures and encryption should already be there before any transfer because it's an obligation under Article 32 of the GDPR. Pseudonymisation is also mentioned a lot of times in the GDPR but as a measure it should be applied *before* any decision to transfer. Pseudonymisation and encryption are not the solution to transfers: they should already be in place before any transfers. They can help you to justify, for example, a change of purpose or evaluating the risk for DPIAs.

From this perspective, they should not be viewed as “additional measures” so much as “primary measures” under the GDPR. Regarding anonymisation, if you don’t need to access the original data anymore, it should be anonymised.

Mark Webber (Fieldfisher): If we are too prescriptive, we end up with prescribed localisation. We are now in a situation where Schrems II is making us focus on SCCs, but there are other potential transfer methodologies out there if we get more creative. Encryption, anonymisation, Pseudonymisation are all things we should be thinking about but we shouldn’t be narrowing down to any one or several solutions. I think it’s our duty to help businesses make up their mind around which one or several is right for their situation.

Anonymisation does remove us from the GDPR. But it is difficult to do and I think we can discount it in most situations since true anonymisation removes data utility. In addition, data that might be anonymised today probably won’t

remain anonymised in 3 or 4 years' time given the increasing capabilities of computing and ongoing advancements in technologies.

Encryption is almost always a prerequisite. But when we do talk about encryption, we need to be careful. There's encryption at rest and there's encryption in transit: different types of encryption protect against different things. We have to be careful that we're not forgetting what privacy means. Privacy is not just security. Privacy requires that you also protect the data when it is being used.

I think Pseudonymisation is very powerful and businesses should be thinking about it. It's a useful tool in preserving identity, but it is often misunderstood. It's part of our duty to explain that Pseudonymisation isn't just the old way of doing it. In addition, the GDPR requires that the "additional information" necessary to re-link data to identity must be in the hands of the controller. We must be careful however not to assume that the controller is always in the EU. This is not always the case.

Patrick Van Eecke (Cooley): There is no one-size-fits-all solution. In certain circumstances for some scenarios, anonymisation, encryption, and Pseudonymisation could certainly serve the purpose. If you've got anonymous data, you're out of scope of the Chapter 5 of the GDPR on data transfers. But to do that we need to ensure that from a technical perspective, the necessary measures to truly anonymise have been taken into account.

We all agree that Pseudonymisation is not anonymisation. However, I raise the following question: if you Pseudonymise data on EU territory, keep the key on EU territory, and transfer the data overseas to another country where they don't have access to the key, could the country consider that data to be anonymous data since there are no means reasonably likely to be used to re-identify those data? The 63 pages of the CJEU decision are about a company transferring data outside of Europe, and whether you can assure that surveillance authorities do not have the possibility to read the personal data. If you Pseudonymise the data and the controller retains the key in the EU, you could claim that technically, indeed, surveillance authorities would not have the possibility to read the personal data.

John Bowman (Promontory): One of the key points is that we don't know what technology is coming along in the future. There is a big gap between regulation and technology, and as time goes on the gap increases. The GDPR is a principles-based regulation, which cites examples of encryption and Pseudonymisation as data protection or privacy-enhancing measures. They might be the latest and greatest now, but something else might come along which is better.

Having said that, any data controller or any data exporter needs to look at the menu of measures which are available to them *now* and consider them in the context of the processing that they're currently doing. For example, a life sciences or a pharmaceutical company might consider that it's important to share the results or the data of their research to other laboratories around the world. COVID is bringing this question to the forefront. There might be benefits to all humankind in terms of that data being accessible because it's a global problem. But they need to think about what safeguards are available already. It certainly may be sensible to think about the secure environment in which the keys necessary for GDPR-compliant Pseudonymised data are kept.

Obviously, we're still awaiting guidance from the EDPB. But, in the meantime, do everything you can to protect data and ensure that appropriate safeguards are in place.

Q3

Panelist Question:

How realistic is a strategy based solely on data localisation, given the broad definition of transfer, which includes not only processing outside the EU, but external access to data stored in the EU?

Anna Buchta (EDPS): I would say that it might be a realistic scenario in some cases. At EDPS we have identified situations, types of data, types of processing that in our view should not be transferred out of the EU or out of the EEA. There might be situations where this should be the preferred course of action but that does not mean that we would support a general argument towards data localisation.

What we want to achieve is compliance. We are committed to working with our partners in the EDPB towards such understanding of the implications of Schrems II that would still leave a possibility for transfers to as many jurisdictions as possible, provided that compliance with the Schrems II Court judgment can be ensured.

Romain Robert (NOYB): I fully agree with Anna. As far as I remember in the EDPS statement in the paper in July, the data location principle was encouraged by the EDPS but not suggested as a rule. I think it should also be considered whether the transfer is necessary. Another issue that is sometimes mentioned is what about US companies based in the EU that could be subjected to the FISA or Courts? Nobody has the answer to this question.

I want to raise one further issue. It's nice to have Pseudonymisation or encryption techniques and everything. But what about the judicial redress that the Court already raised as a fundamental right of the holder of the rights in the EU? How do you create a judicial redress with contractual clauses?

We have to learn the lesson of the Court this time. We had a Schrems I. We had a Schrems II. I think we don't want a Schrems III. I think the Court was clear.

John Bowman (Promontory): I think data localisation is a matter for those businesses who have international footprints: understanding their data flows, where the information is going, what safeguards are in place.

Clearly, Privacy Shield was considered to be insufficient in providing those appropriate safeguards. But SCCs survive to live another day. Appropriate supplementary measures should be put in place, and organisations can start thinking about what those are. We await the guidance on that. Hopefully, once the guidance is clear, then the companies can work out what's the best for them.

Patrick Van Eecke (Cooley): I do believe that localisation or relocation should be part of the exercise. It's part of the menu of the different measures that organisations should be taking into account. The only concern I'm having is that localisation could lead to balkinization. I'm concerned about global businesses where, for example, you've got an HR Director who has EMEA (Europe, Middle East, Africa) responsibilities. Maybe today that HR Director is based in Dubai, but in 2 years, another HR Director could be based in Australia. When that person has access to data on servers based in Europe, it's seen as a data transfer. This is the kind of horizontal cross-border kind of data transfers that we see at a global level. Companies have always got to be confronted with their needs for transferring personal data.

Q4

Panelist Question:

Can companies just rely on assertions by US cloud providers that their SCCs make processing there compliant?

Magali Feys (Anonos): I don't think so. I think that additional safeguards are also required. The whole question about the territorial scope of FISA and all comes into perspective.

Romain Robert (NOYB): I would like to refer to the "Next Steps for EU companies & FAQs" available on the NOYB website. It was suggested to SMEs in the EU to ask their providers. Some people are struggling but I don't have much empathy for companies who don't even provide an answer to the question. They're not even trying to find a solution.

Anna Buchta (EDPS): There are very high expectations towards the regulators to provide clear, harmonised, practical, bulletproof, court-proof Guidance. We are very aware of the difficult predicament most businesses are finding themselves in. There is a lot of hard work going into providing this Guidance as soon as possible. I would encourage people to have realistic expectations around this. There are obvious interconnections and interdependencies between any guidance on Schrems and supplementary measures, and what the new SCCs will look like. It's crucial that these two processes are aligned.

Please be patient. We are doing our best. But nothing we do will remove the baseline of the GDPR principles, including that of accountability. This means that every controller has to take steps by themselves and apply measures *now* which are necessary to ensure compliance with the GDPR, including the provisions on transfers.

Further Enquiries

Anonos is committed to discussion, collaboration, and education in the field of data privacy protection and data use, including legal developments, regulatory changes, and the use of technology for ethical, lawful, and socially beneficial purposes.

Further education opportunities are always on our radar. You are welcome to reach out to us with any questions or comments that you might have about the Schrems II webinar summary and FAQs above, or any related enquiries.

Please also feel free to get in touch directly with Gary LaFever, CEO and General Counsel of Anonos, and moderator of the Schrems II panel, at gary.lafever@anonos.com.

If you want to learn more about Anonos and our solution, take a look at anonos.com, or contact us at LearnMore@anonos.com.