Schrems II - Lawful Data Transfer Webinar

Webinar Transcript

8 October 2020

Discussion on how **Additional Safeguards** enable lawful data transfers using SCCs & BCRs.
Video replay from the webinar can be viewed at: **SchremsII.com/learn**

SPEAKERS

Romain Robert
NOYB

noyb

Anna Buchta
EDPS

EDPS
European Data Protection Supervisor

Patrick Van Eecke
COOLEY

Cooley

John Bowman
PROMONTORY

PROMONTORY

Mark Webber
FIELDFISHER

fieldfisher

Magali Feys
ANONOS

ANONOS

MODERATOR

Gary LaFever
ANONOS

ANONOS

Gary LaFever
ANONOS

ANONOS

Gary LaFever (Anonos)

[01:46]

I would like to welcome everyone to this webinar on Schrems II Lawful Data Transfers. I would like to share with everyone that we have over 2000 registrants for this event and registration only opened up 72 hours ago. I think that's a reflection of the reputation, respect, and expertise of our panelists, and also the timeliness of this issue. So, I want to thank all the panelists for taking 2 hours out of their day to participate on this webinar and also to all of you. We do believe it's going to be worth your time, and we also want to encourage you to submit questions. All registrants will receive by Tuesday of next week, a recording of this session. And by the end of next week, we will get the FAQs back to you as well.

And so, I'd like to introduce myself and give you a little overview and background on the purpose and focus of this webinar. So, my name is Gary LaFever. I am the CEO and General Counsel of Anonos. Anonos is a technology company that for the last 8 years has been doing research and development in balancing the interest of data subjects and consumers with the legitimate business interest of companies and organizations and even governments. And obviously, you may ask: “Well, 8 years? The GDPR wasn't even around.” But the GDPR is the newest incantation as it were of fundamental data protection principles. So, when we set out to develop technology, we were looking at the Fair Information Practices. We were looking at the OECD guidelines. And obviously, we keep abreast and are actively participating as new measures and techniques and standards evolve.

Anonos is a technology company. But this webinar is not about technology. And so, I want to explain why this webinar was put together. It's because there are a lot of discussions about Schrems II. It's a very topical, very timely issue. There are a lot of concerns. There are a lot of interests. But a lot of it deals with other topics, and it's not those topics that we will talk about today.

So, this is not about whether the Schrems II decision was a proper decision. The fact of the matter is it is a final, unappealable decision by the Court of Justice of the European Union. It's unappealable. It is the law. And so, we're focusing not on technology, but we're focusing on legal principles and we're going to use a fact pattern - all of us so that we have a focus here. This fact pattern is an EU Data Exporter who is looking to comply with Schrems II. They don't want to engage in regulatory arbitrage. That dirty word that people never say out loud, but they think. They want to do it right. They're looking to comply with Schrems II while still conducting business.

And there are a lot of questions that can be asked as the appropriate lawful approach to conducting international data transfers. But for this purpose, we're concluding that the SCCs are the best approach. And then, we are looking at the three potential additional measures, additional safeguards that had been identified so far as the only ones and it's from the German DPAs - encryption, anonymisation, and Pseudonymisation.

So, really, you can look at this as there are two questions. The first is: "**Is it actually possible to comply with Schrems II and still conduct business?"** But I actually think the better question is: **"Can complying with Schrems II actually provide you a competitive benefit?"**

As you all noted, this webinar is being hosted on Zoom. We had numerous emails about: "How can you select Zoom when they're not compliant with Schrems II?" But then, we had other emails saying: "We don't think any video conferencing system is compliant with Schrems II." And we even had some people tell us that as much as they wanted to attend this webinar, they have corporate restrictions on the use of Zoom because of privacy and security concerns. So, this is why I raised this as a competitive benefit. Imagine the competitive benefit that a video conferencing service that could show they were Schrems II compliant would have.

And so, that's the backdrop for this webinar. If you came to this webinar hoping that we'd have a philosophical discussion about the need for political solutions, you're going to be disappointed. It's not that that's not a critical point. In fact, I think the long-term solution here requires politically addressing the issues at hand, but we believe what we're talking about is something that's not getting airtime and that's our focus.

So, a couple of background principles. Some of this is going to be background for all of you, but we're trying to set the stage. The first is Data Protection by Design and by Default. It is something that is mandatory for all processing. It's not optional. And why is it mandatory under the GDPR? Because contracts aren't enough anymore. Contracts aren't enough anymore because when a contract is breached the data subject - the consumer typically has no redress. And so, the GDPR, for the first time, created a heightened version of Privacy by Design and said you must do this by default. So, what does that mean? Well, it means that as soon and as often as possible you should de-identify the data and I'm purposely using a term that does not exist under the GDPR, de-identification, because I wanted to be as broad as possible.

So, you're supposed to de-identify as early and as often as you can. And this raises Pseudonymisation. Pseudonymisation under the GDPR is not everything it was before the GDPR. Pseudonymisation has been around for decades. It means very different things. But Article 4(5) of the GDPR only identifies a heightened level of Pseudonymisation where it is impossible. If

you satisfy the definition of 4(5), it requires that it would be impossible for someone to go from identity or on this slide what we're showing as Who related to an individual versus the What data that could relate to multiple individuals.

And so, the question that hopefully you get an answer to or at least have a different perspective on by the end of this webinar is whether or not these additional measures could allow an EU Exporter to conduct business in a way that's compliant with Schrems II, in a way that would be impervious to surveillance by external countries.

Panelist Self Introductions:

So, with that, we're going to introduce the different panelists and allow them to give their background on Schrems II and also to provide information regarding their particular perspectives. Anna, if you would please start.

Anna Buchta
EDPS

Anna Buchta (EDPS)

[09:20]

Thank you very much, Gary, and welcome everyone. It's a true privilege to be here with you today to discuss this very topical judgment and its consequences. So, I am the Head of Policy and Consultation for the European Data Protection Supervisor and that is the independent data protection regulator for the EU institutions and bodies. So, in addition to supervision, we also advise the European Commission on various initiatives related to data protection, and we are also a member and provide the Secretariat to the European Data Protection Board. You may have heard about this. This is the relatively new body that brings together all European Data Protection Regulators.

And as you no doubt know, the EDPB has already issued an FAQ document about the follow-up to Schrems II judgment immediately after it was released in the summer. And since then, we have been working on further guidance, in particular on the supplementary guarantees that in the Court's view might be necessary to supplement the Standard Contractual Clauses to allow transfers to non-adequate jurisdictions. Unfortunately, the guidance is not ready yet. Of course, we are doing everything we can for this to be published soon

But I wanted to mention that because I hope it will also explain why for me today it will be very difficult to speak at any level of detail to what the regulators might ultimately decide in this context. And so, obviously, I cannot speak on behalf of the EDPB and what I will say here today should not be taken as an official position of the regulators. But very much looking forward to this

discussion about the seminal ruling of the Court of Justice and how to go about its consequences in practice.

Gary LaFever (Anonos)

[11:40]

Fantastic. Thank you. And next, Maggie.

Magali Feys
ANONOS

Magali Feys (Anonos)

[11:48]

Thank you, Gary. First of all, I also would like to say it's a true honor to be on this panel and really looking forward to the discussion. My name is Magali “Maggie” Feys, and I'm a European IP, IT, and Data Protection Lawyer and I serve as the Chief Strategist of Ethical Data Use at Anonos and I'm also the founder of a boutique law firm, AContrario. I also am a member of the Legal Working Party, e-Health, for the Belgian Minister of Public Health and I'm currently drafting a PhD on the secondary use of health-related data.

With regard to the Schrems II decision, I think that it was a necessary decision that had to be made by the CJEU because they had to take a position definitely in accordance with the US Government surveillance laws. But whilst the conclusion of the CJEU was that additional measures are necessary next to the SCCs in some cases for international data transfer as Anna already pointed out, as of today, they are not really defined, which leaves companies with a gap in dealing with or processing and transferring data with US companies. And as Gary also pointed out, they want to comply but given that there is not a real solution and the guidelines are not yet ready, that leads to an uncertain situation. So, I hope that you'll allow me to just take my introduction time to present the Data Embassy Principles.

We submitted them to the EDPB on the 29th of July as what we think could be a potential, lawful supplemental measures under Schrems II because Data Embassy Principles really have the means to maximize the lawful and ethical for example secondary processing of personal data like data analytics, AI, and machine learning, but also international transfer of data. And they do so by enforcing established EU Data Protection principles to satisfy the safeguards that were mandated, or the additional safeguards mandated by Schrems II.

If you want to review them, they are on DataEmbassy.com. And the five Data Embassy Principles as shown on the screen are the following. The first one is the heightened level of Pseudonymisation as defined in the GDPR. So, it means really enforcing Pseudonymisation, which is in line with the guidelines

as established by ENISA and it's a technical enforcement actually of the basic principles under GDPR and that also allow for functional separation, which was one of the recommendations in the past by the EDPS. And given that it really was put in the GDPR as a heightened level that it comes back as a concept and an outcome rather than solely a technique. We think it could be very appealable to the EU Supervisory Authorities.

The second principle is Data Minimisation, which is one of the basic principles under Article 5 of the GDPR and by enforcing what is already pointed out by Gary of the principles of Data Protection by Design and by Default. The third principle is then Secured Personal Data. This really means restricting the processing of your personal data to a form of personal data that does not enable the identification of data subjects without that access of that additional information, which is then necessary for the relinking, and you really keep that additional information in the sole possession of the EU-based Data Exporter.

The fourth principle is then Demonstrability. The proactive technical enforcement must really enable data controllers to really show the fact that they are compliant with the principles under GDPR and the accountability principle. And the last principle is responsibility. Also, once again, by really embedding technical and organizational measures in your company in the data flow in the data processing, it definitely enables data controllers to demonstrate their compliance.

I really want to note the Data Embassy Principles are propositioned as a solution to the EDPB but they're definitely not a silver bullet and they may not work in every situation. We are well aware of that. But they can really provide a valuable option for processing personal data using cloud, SaaS, and outsourced services for global transfer outside the EU as such. Thank you.

Gary LaFever (Anonos)

[17:41]

Thank you very much, Maggie. Romain, would you please give an introduction to yourself and the work that you have done that the NOYB is involved in?

Romain Robert
NOYB

Romain Robert (NOYB)

[17:49]

Sure. Thank you, Gary. Thank you for having me and good afternoon/morning/hello to everyone. We are in different time zones, I guess. So, my name is Romain Robert. I'm working for NOYB. For those who don't know what is the meaning of NOYB, it stands for None of Your Business, which gives a little bit of explanation of what NOYB is doing.

Basically, NOYB is an NGO based in Vienna created 3 years ago by Max Schrems, a quite famous activist in the field of privacy that was the origin of the Schrems I Decision and of course the last decision in July. NOYB is composed of 9 lawyers. We are a team of 9 lawyers right now and 15 staff members in total. I think we are approaching 4000 members by the end of this month.

We were quite involved as well in the follow-up of the judgement intervened by the Court of Justice in July with two main follow-ups. The first one was the one that we initiated in Ireland against the DPC or the Irish DPA trying to implement the judgment against Facebook because Schrems I and II are also about this very specific controller. Not about all controllers but about Facebook in the first place. So, the first objective of note was of course to enforce this judgment against Facebook in the Facebook case since it was the origin of Schrems II Decision.

And we also tried to implement the judgment of July with the so-called 101 complaints that we filed against 101 companies across Europe in 30 jurisdictions, and we are still waiting for the answers of the DPA. We have to correct some bugs because apparently, we had some problems with the complaints that we had to rectify. So, that's the other actions that NOYB was taking to try to implement the judgment in these respects. In this case, the complaints were concerning Facebook and specific Facebook Connect products transferring data to the US and also the Google Analytics service that was used by the websites against which we filed the complaints. So, that's the follow-up action that were taking by NOYB so far.

And of course, we are still concentrating to file other complaints or just to take further actions to go further with the judgment and Schrems II of course in order to avoid to end up another time before the Court of Justice to have a Schrems III. So, I think nobody wants to have a Schrems III and I think we are the first one to try to avoid to go back to the Court of Justice to have another decision to confirm that was already said twice by the Court of Justice. So, that's a little bit of the state of play here in Vienna.

Gary LaFever (Anonos)

[20:59]

Thank you, Romain. Mark, if you would, please.

Mark Webber
FIELDFISHER

fieldfisher

Mark Webber (Fieldfisher)

[21:03]

Of course. Good morning. Thank you, Gary. Good to be here and thank you for your invitation. So, I'm Mark Webber. I run the Silicon Valley office for Fieldfisher out on the West Coast. It's just becoming light out here. So, in reference to time zones, really quite relevant. I'm a Brit and an English and European lawyer, but I practice my trade out west. And really, for 20 years, I've been a technology lawyer. I've spent an awful lot of time in privacy. And while Fieldfisher represents businesses from all across the spectrum, the majority of my office spends time working with US tech vendors, particularly those in cloud and SaaS, and particularly many of those who have customers which are impacted by this decision and have therefore impacted themselves both in terms of their own operations and supporting the needs of their customers. So, we've really been acting in the middle of this since July and before because, obviously, everyone had a keen eye on what the Schrems II decision was going to say.

I think it would probably be fair to say that we've had to be pretty agile and creative in the last few months. We've already heard other panelists refer to this sort of vacuum. We're waiting for further guidance. We've had some comments from Germany and the regional regulators, which are helpful but also unhelpful in terms of consistency. The thing with the vacuum is as soon as somebody says something, everybody jumps on it. But it's not necessarily the final conclusion and it's not necessarily a consistent conclusion, it makes it very difficult for exporters to determine what they should be doing and importers to be reacting to that.

I think the one thing I will say just to sort of open up is I've been incredibly pleased by how seriously the various parties are impacted by this decision and have been taking the data transfer situation. Putting aside frustrations with the changes, everybody's working hard to come up with a solution and to come up with safeguards and focus on the objective risks that are involved in relation to data transfers before and since this decision. I think what we're doing really as a firm and working with clients is twofold trying to respond to customer inquiry and customer questions about data transfers and the way data is protected. But then introduce and explain safeguards that may be deployed in relation to protecting data when it's being transferred.

From this introduction to the panel, we can already see from the players in the market those safeguards are going to be necessary. I don't think anyone's arguing that SCCs alone are enough anymore, but it is going to be a combination of safeguards and coming out with the right kind of safeguards focused on risk, not losing sight of the actual risks, and what you're trying to protect, but also layering up those protections and discussing how those

protections work one in the light of the Schrems decision and secondly in the light of what the regulators may see. But also, thirdly in terms of what's practical and what's actually possible because this is all happening in the backdrop of the COVID recession. Businesses are struggling. Individuals are struggling.

I, for one, am very serious about privacy, but I don't want to see this lead to more localisation, less use of the internet, and less use of technologies which will change our worlds. I think the majority of people on this conference call have survived in COVID because of their ability to turn to the internet, and the internet is a great game changer for all, and I think we've all got a role in making sure we can continue to use those technologies and work with those businesses too for the good of everybody. I think being creative and working together to do that is where I think it has helped.

Gary LaFever (Anonos)

[25:16]

Thank you very much, Mark. I think you're right, I think we can all relate to the need for interconnectivity. As you point out, not at the cost of loss of personal rights. So, with that, Patrick, would you please pick up and introduce yourself and your orientation to the subject?

Patrick Van Eecke
COOLEY

Cooley

Patrick Van Eecke (Cooley)

[25:33]

Sure. Thanks, Gary. And good afternoon everybody. Good morning to the West Coast people and East Coast in the United States. It's a real pleasure to be here together with you and especially discussing this very hot topic. I've been active as a lawyer for the past 25 years now in the field of privacy and data protection. And actually, I just looked it up. I started at the same month as the Data Protection Directive got adopted. So, there must have been something that brought us together.

And data transfers, as you may know, they were already in that Data Protection Directive 25 years ago. So, not too much has changed since then. But of course, now, today, we are really confronted with this kind of challenge. And as you Mark already mentioned, we as lawyers we really want to try to find solutions because clients and companies are coming to us asking for a solution, not tomorrow, not next week, but today because what we really understood from the Court of Justice and any further guidance coming out of it is the monkey is now on the shoulders of the companies. It's up to us to do

an assessment of the equivalence or the adequacy of the legal regime in so many other countries outside of the European Union.

And secondly, it's also up to us to come up with remedies for sure, which we're going to discuss in a few minutes. And these two points we also have seen in practice over the past few months now being at Cooley and working with so many clients. These are the two most important challenges we are currently seeing with the companies and clients. One is: “Oh, but we thought that you just take a map of the world and you color some countries red and orange and green, and then you know to which country you can transfer or not.” No, not true. Because the Courts - it's 63 pages. I know it's difficult to read. But that's the good thing about lawyers. We digest this for you. And so, we can bring that kind of information to you. But the Court is very clear on that that it's an ad hoc assessment. You can't just say that country is a no-go zone and that other one you can go to. No, it depends on the type of personal data. It depends on the purposes. It depends on the data subjects or the people whose data you're actually processing and transferring. So, it's always a case-by-case assessment that needs to be undertaken. And that's a difficult challenge, isn't it?

And the second challenge that we see companies are being confronted with is the solution. Wouldn't it be great to have a one-size-fits-all solution for this kind of data transfer thing? No. It's not true. It really depends. We know there's going to be this kind of magical mix of technical measures, organizational measures, contractual kind of announcement, and these kinds of things properly combined they will be able and they will allow us to transfer personal data in a way that we as companies can say: “Yes, we've done our homework. Yes, we are responsible for that. And yes, we are accountable for that. So, we can show you that we have done this type of work and taking a risk-based approach.”

It's a huge work. I know many of you, you're at this moment already 1200 people are participating, which is amazing. Actually, it's a very difficult job and we should do that as efficiently as possible. And over the past few months now at Cooley, we've been able to - I don't want to make a commercial of it. But I just wanted to mention to you because probably many other organizations or law firms are doing the same thing. But I just wanted to share with you that knowing that it's a risk-based approach, knowing that it's all about accountability, namely showing that you've done what is necessary, well, we believe that it's all about consistency.

And so, we developed a kind of methodology. It's no rocket science, but in different phases and using a methodology and having a methodological approach towards this issue and a documented approach that actually brings us very far already in this kind of exercise. The methodology is supported by a tool, a kind of product. We use kind of an algorithm for doing the

assessment, and then coming up with a proper kind of remedy, some kinds of suggestions.

What we noticed is that by using such kind of a tool, you take away this kind of subjective discussions spending hours of time sitting around a table. What do you think? Is that country sufficiently adequate or not? What do you think? No. You're able to objectivize it. And so, then you can start thinking about solutions. So, being solution oriented. So, that's what we actually have been doing, Gary, over the past few months since the 16th of July actually and even before because I think we all felt that the Court was getting ready to decide into this kind of direction so we started to prepare ourselves a bit earlier.

Gary LaFever (Anonos)

[30:54]

Fantastic. Thank you very much for that, Patrick. So, John, would you please round out the introductions by the panelists with your perspective and the orientation of Promontory?

John Bowman
PROMONTORY

John Bowman (Promontory)

[31:04]

Thank you. Thank you, Gary. And thank you to fellow panelists as well. Fantastic round of introductions already, and I think most of the team here have covered some of the points I wanted to raise, but that's okay because at least it shows we've got some consensus on the key issues. There's no doubt that Schrems II is a landmark judgment. You can see that from the number of attendees at this session, which I think is rising as I see on the ticker on the right hand side, which is great.

This is a bit about me. I work for a company called Promontory, which is a consulting firm. I've been there for 6 years. We help mainly sort of large global organizations comply with the data protection laws, and we have a global practice in the UK, the US, and other sites across the world. Obviously, our experience over the last few years has been largely GDPR related, certainly in respect of our European business. But of course, the sort of focus on purely GDPR compliance is kind of fragmented to some extent now and new and exciting issues are arising like AI, machine learning, digital ethics, as well as the new sort of legislative frameworks, which are emerging like CCPA, LGPD, and many others of course. And, of course, data protection is becoming a global concern and rightly so.

I think Schrems II is pertinent in this context because it sort of addresses too the fundamental objectives I think of the GDPR. One is to protect personal

data. That is an EU fundamental right. So, every person and every data subject in the EU has the right to the protection of personal data, and I'm reminded of that by this miniature version of the EU's Charter of Fundamental Rights, which I think is a legal document I'd highly recommend to everyone. On Article 8, there it is. You can see it. It's perfectly legible. The Fundamental Rights is a key aspect because we can see from all the landmark judgments everything from the Privacy International judgment yesterday about retention of telecommunications data, the two Schrems cases - Schrems I and Schrems II, the repeal of the data retention directive way back in 2014, and even the right to be forgotten judgment. The Fundamental Rights is at the heart of that. And of course, the GDPR and the Charter says that everyone has the right to protection of personal data.

Another objective of the GDPR though is to facilitate the free flow of data. And, you know, it's all about a balancing act. Free flow of data provides benefits to society and to individuals and to businesses and that must not be forgotten. So, I think what Schrems brings into focus is effectively the kind of tension between on the one hand the fundamental rights and protection of personal data and on the other hand the societal benefits that the free flow of data can give. But I think we can all come to our own conclusions as to which side of that sort of balancing act the pendulum is swinging to some extent.

I think looking at GDPR, there is a general prohibition on data transfers unless there are certain mechanisms or measures in place, and one of those is the adequacy decisions. Normally, these take a number of years. There are a handful of regimes In the world that have adequacy decisions. They are subject to intense scrutiny by the European Data Protection Board, the European member states and so on. But one of the novel aspects, I think of the Schrems judgment is that data controllers or data exporters alongside the recipients are obliged to some extent to make those adequacy determinations themselves ineffectively in effect by assessing the risk that posed to the data when it's transferred to in European terms a third country. Of course, this is a pertinent issue here in the UK.

The UK is currently going through an adequacy negotiation with the European Commission. At the moment, the timing is tight, the clock is ticking down, and really the adequacy decision needs to be in place by the end of this year. Otherwise, data exporters from the EU transferring data to the UK will have to take into account all the Schrems measures, as well as having the appropriate safeguards in place whether that's SCCs, binding corporate rules, and so on. So, I'll leave it at that at the moment. But I think, hopefully a fascinating discussion to come.

Gary LaFever (Anonos)

[36:18]

Thank you very much, John. So, I just want to take a second here and explain to everyone we've had quite a few people joining recently that this webinar is going to be in two sections. The first section is going to be three questions, which each of the panelists will answer. And you will have an opportunity in real time polling to answer as well. After those three questions, then we will take audience questions. So, please continue to submit the questions that you have.

So, let's start with the first question. And this question is the one that the audience is going to be asked to answer. It is slightly different from the one that the panelist will answer. And you will get this polling at the end of the answers from all of the panelists. The question is: **Do GDPR obligations of Data Protection by Design and by Default extend beyond international data transfer situations?**

Panel Question No. 1:

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, would you like to lead off please?

John Bowman (Promontory)

[37:59]

Well, that's a great question, Gary. I think, well, Data Protection by Design and Default is one of the articles in GDPR and really applies to all data processing activities. So, it's something which has to be baked into any organization's approach to designing applications, designing services, ensuring that their data processing activities are safe, they're lawful, they're transparent, go into all the usual and familiar data processing principles, which are set out in the GDPR.

Data Protection by Design and by Default is an interesting concept, which has been around for a number of years, but it's great I think that it was incorporated into the GDPR and effectively had legal effect. Now, what can organizations think about when they're applying those principles? Well, a lot of it's down to the design. You certainly don't want to design a product or a

service and have it redesigned or re-engineered just before its launch. That's obviously going to be costly and cause a lot of disruption to the business.

I mean, in terms of the data transfers, though, clearly, there are measures which can be put in place to sort of help provide safeguards in terms of those data transfers, particularly if they're going to a regime where potentially there are sort of legal and regulatory safeguards or even sort of constitutional safeguards that are necessarily there in place to protect the data of data subjects in the EU, and those can be technical and organizational measures. The GDPR does sort of give the examples of Pseudonymisation and encryption as measures which can be applied.

But generally, the GDPR is technologically neutral. And really, it's all about setting risks and working on outcomes. So, clearly, you want the best risks and the best outcomes. And I think in that situation and that context at least, it's important to sort of focus on the data processing principles, which can be supported by these technological sort of solutions. So, those would be things like data minimisation, storage limitation, purpose limitation, and so on. So, a focus on those principles and an eye to the sort of technological measures which can be put in place in combination will help sort of safeguard the data in transmission and once it's received by usually the data processor, but whichever party's receiving the data.

Gary LaFever (Anonos)

[41:01]

Thank you, John. Patrick, would you like to respond to that question, please?

Patrick Van Eecke (Cooley)

[41:05]

Sure. I don't want to repeat, John, what you just mentioned but I fully confer with you that Data Protection by Design and Data Protection by Default are core principles of the GDPR and they're applicable always. Of course, how you do it in practice, that's the difference. But the principles they apply, I would even say that it's a mindset. It's not a process. And maybe just to give you just a small secret, how did that actually end up in the GDPR? Well, at that moment, Viviane Reding, the commissioner of DG Justice, was visiting one of the German car manufacturers and they got confronted with an issue where they were all working on connected cars. The legal team as it so often happens they only come at the end of a kind of assessment relating to: “We’re going to roll out these connected cars next week and you need to sign off, Legal.” So, this happened as well with the car manufacturer. So, what

happened? Well, apparently, whenever you would with your smartphone, you would connect to the car the data would be uploaded to the hard disk of the car but it will also go immediately into the cloud without taking into account consent mechanisms, etc., etc. So, the context database would immediately be in the cloud operated by somebody else.

The legal team on the 9th floor of the German car manufacturer then said: “But you can't do that. We actually need to make sure it is data protection compliant.” The engineers at that moment said to the legal team: “Too late. We can't do it any longer. We need to go back to the drawing board if we are going to have to make such changes. It's already baked into the software and into the hardware.” That's the moment that the Luxembourg DG Justice Commissioner figured it out and said: “We need to do something about it. We need to make sure that not just the lawyers but also the engineers and the developers start to think about privacy already at the drawing board.” And that I would say that's the main message. It's a mindset. It's not a process. And once we've got that embedded within an organization, many issues will be solved.

Gary LaFever (Anonos)

[43:26]

Great perspective. Thank you for that, Patrick. Mark, please, if you would provide an answer to that question.

Mark Webber (Fieldfisher)

[43:32]

Sure. So, thank you. Building on what John and Patrick have said really, I think the heart of these core principles of the GDPR, they apply whenever you’re processing personal data. The definition of processing is very clearly wide and very clearly applicable whether you’re processing in a small church group in Sweden or you’re a large organization acting on a global basis. So, there are still principles that have to be reapplied. But there are always these elements of proportionality and assessment. And of course, the GDPR is principle based and principle based for a reason. One, so we can evolve technology and still apply state of the art and actually in dealing with Privacy By Design, GDPR asked us to look at state of the art. So, what's accessible at the time, and that would also be partly based on what's accessible to the organization in question.

We can't hold every organization to the same kind of standards. Yes, there's a minimum level of standard, but the large corporate with millions to spend on

IT and security is going to have more state of the art accessible to them. So, the appropriate technological and organizational measures that they may bring to a processing solution are going to be different. And I think coming back to that proportionality, Data Protection by Design and building into Default talked about only processing data that is necessary. So, that's the key point. And I think we should certainly come back to this when we talk about the operational safeguards that we'll talk about because as I mentioned in my introduction it's about a combination of solutions. And of course, it could be not processing the data at all. And we'll go on to talk about anonymisation. Brilliant! Anonymisation takes yourself out of the GDPR. It's not actually practical in many situations. Businesses need data. Individuals need to communicate in email. So, there is often data which has to be transferred.

What we're really saying is don't make available data on an unlimited basis to individuals. There are some kinds of restrictions. And as a part of Data Protection by Design and Default, we're asked to then think about policy and implement policy in relation to the handling of that data. And again, that becomes a layer of protection alongside contractual, alongside other types of safeguard. So, yeah, I absolutely agree. It matters. It's a fundamental element. I like Patrick's idea that it's a mindset. I think it is. But it's also about proportionality. And again, as I say, focusing on the objective risk. What kind of danger is this? What kind of things are we protecting? And then, how can we protect that? Sometimes we need the data. Sometimes we might be able to use the data in an encrypted or pseudonymised format. But sometimes we might need it in the clear. And we've got to understand that and in a proportional way, work out what makes sense in context.

This all comes back to the burden of accountability sits with the controller, and the controller needs to be thinking about that and what they need to do with data. The difficult part of Privacy by Design is it's a controller obligation. It's not a processor obligation. And I sit there working with many, many vendors out there who are going to be acting as processors. They're anticipating what their controllers need. So, always, by default, processors need to anticipate Privacy by Design because they need to design products, put things on the market that individual customers will want to buy. But there's a level of difficulty there as well because what somebody's view of sufficient is and what somebody's view of proportion is isn't necessarily the next customer's view of sufficient and proportionate. And that's one of the inherent tensions that we deal with with things like Privacy by Design - different interpretations, different guidance, different circumstances, and different appetites for risk.

Of course, no controller has to take the processor's services. They're there. They're available. But that's also part of this discussion, and we've been talking about making the evaluation of what data is being transferred. Of course, one of the other accountability principles is taking an evaluation of the

third parties or subprocesses you rely on, which is another element of this, which I'm sure we will go on and talk about.

Gary LaFever (Anonos)

[48:04]

Thank you very much for that, Mark. Romain will go next. But before he does, I would like to ask everyone, I know it may be tempting at the top of the hour to leave. But at the end, after Romain, Maggie and Anna, give their response to this question, we will have our first live polling to see what the audience thinks. And just so everyone knows, in 72 hours, we had over 2300 registrants for this event and roughly half of you are currently live. So, to be able to see not only what the experts on the panels think on these topics, but to see what your colleagues think as well, we encourage you to stick around and participate in that live polling. With that Romain, please, we would love for you to help answer this question.

Romain Robert (NOYB)

[48:48]

Thank you, Gary. Yeah, of course, I would agree with the panelists that of course the Privacy by Design and Privacy by Default are transversals. They are not only applicable to transfer that's for sure. There is no specific situation when they should be applied. With that being said, I would also like to say that Data Protection by Design and by Default is also a nice principle, not only to mention but also to apply.

Let me give you an example on transfer especially with the 101 complaints that we filed last month. Some of the controllers that we filed a complaint against used Facebook Connect and Google Analytics products. We already had four controllers - two in Romania, one in Amsterdam, and one in Luxembourg if I'm not mistaken who came back to us saying: “Oh guys, we didn't realize we were using Facebook Connect and Google Analytics. Then, we removed this product and services on our websites.” And I think that is Data Protection by Design and by Default. That's a nice application.

So, it's nice to mention that it should be applied. But I guess that all people professionally and privacy experts and especially as an expert will advise the clients to actually implement Data Protection by Default and by Design in reality and actually to remove everything which is not necessary for the services. So, this Facebook Connect and this Google Analytics were removed by the websites that were targeted by the complaints. And in this respect, we have now decided to withdraw the complaint as well because the aim is not

to obtain a fine or to reach a fine at any cost. So, that I think is a nice application and a nice example of Privacy by Default and Privacy by Design.

On a final note, I think it's also interesting to mention that Privacy by Default and Privacy by Design is not a way out for transfer if a transfer is illegal. But it's a nice way to, for example, diminish or decrease the level of the fine, which is one of the elements that might be taken into consideration and that should be taken into account by the DPA when determining the level of the fine. On a final note, I understand a lot the risk-based approach. I think, it is really appealing for businesses than nothing. But I also sometimes kind of in a standard this kind of respective approach is understood as long as we've done everything that we could, it seems that we have found a way out. And sometimes I also understand that people just understand this principle of risk-based approach and accountability as: “Oh, it seems that the only things that are transferring to us, it's just a couple of cookies and it seems to be okay.” It's not my reading of the GDPR to be honest. It's not how I see the risk-based approach. You have to take all measures to limit the risk of privacy. But if you're still aware that data are transferred to the US illegally meaning outside of any SCC or transfer to a company, which is subject to an NSA order or FISA order and everything even if it's a couple of cookies, and you minimize like this data minimisation the risk. According to me, it's still a transfer, which is illegal. So, this risk-based approach and this Data Protection Privacy by Default and Privacy by Design principle are not your way out in these cases.

Gary LaFever (Anonos)

[52:24]

Thank you, Romain. That's very insightful. Maggie, please, if you could please respond to this question as well.

Magali Feys (Anonos)

[52:30]

Okay. Well, first of all, I'm going to start saying that I, of course, agree with a lot that has been said already and I really loved having Patrick pointing out that it's a mindset. Because, first of all, that's also something we encounter when also advising companies is that we see that if they already had done the GDPR exercise, a lot of them have done it on a judicial level, the legal level, and they have policies, they have a data register, but they have not embedded those principles that are so beautifully written down in those policies into the technology, into the business system, and into the business processes. And I think if you read Article 25, that's what Data Protection by

Design and by Default is. And as I said, it's a principle going not only to transfer of data but really to the core of what GDPR stands for.

I want to give two sorts of examples because what I think it means for me is when we work with startups and scaleups or for example with R&D departments, and they're really in the innovation, it's as Patrick pointed out. It's from the moment you start determining what you want to do, which functionalities you want to build that you already embed it in the technology, and I think because a lot of people sometimes say: “Oh, GDPR is a contradiction to innovation.” Honestly, I do not believe that. I think that we have a unique position. Or if you are in the innovative industry, in the software development, you have a unique position of not only being innovative with regards to the technology with regards to the blue ocean strategy you want to persevere, but also be innovative in the way you treat data and in the way you protect the data subject’s rights and that it's not only talking to talk but you can also walk the walk.

I can really say that because I've been a front row viewer of a number of US startups and EU startups who have done it. For example, I don't know if you remember Google Home, but Google Home is actually registering entire conversations and they said they needed to train the algorithm in order to improve the Google Home device and the algorithm behind it. And we have been working with Belgian and European AI companies that actually embedded in the device already software that did data minimisation so that only the part of, for example, in Dutch, you have a number of dialects and you could then get confused when they say “Go Google” in order to get those dialects and really get them transcribed and train them the algorithm. So, they are already training the software within the device in order to select that. So, there was always the data minimisation, only those kinds of bits of words of conversations were sent to the cloud and then transcribed and trained for the algorithm. First of all, it was much more valuable data. It was less time you needed from the transcribers because they didn't have to go through the whole entire conversations, but really to the valuable data that was really necessary for the algorithm and they really showed actually next to a Google that they were much more innovative, much more effective to the NLP algorithm. But at the same time, also protected the data of the data subjects. And I think it's a really nice way.

And as already pointed out also by Mark, of course, it's not a one fit for all. For example, companies can work with the zero knowledge principle and that can work for certain companies, for others not. So, you really have to think about how you can define Data Protection by Design and embed it in your innovation. So, I think from innovation, that is very important. On the other hand, of course, it's not only a principle to be implemented in the R&D Department or for startups and scaleups that are developing software, but really also for the businesses. It should really be embedded in the business

processes because I also believe that we are wasting a lot of data. We come from an era where we thought: “Okay. Come give us the data. You never know for what we are going to use it.” And data is being shared without thinking how, why, and when we want to use it. And if I can use an analogy and it's maybe a simplified one, but it's like brushing your teeth with the tap open. At the point you're brushing your teeth, you don't need to have the water. You only need it afterwards to rinse your mouth. And that's really then value for your money.

And so, also with anonymisation, I agree, and that's closing the tap when you're brushing your teeth, but then taking a number of drops of water. The problem with anonymisation really is and I think we'll come to that is that that's the only drops you will have. And if you then for your purposes you need to have more water. Well, tough enough, that's the only drops you're going to get. Pseudonymisation, for example, is the same principle, it opens up the tap. It gives you a number of drops. But if you say: “Hey, today, I'm using a different kind of toothpaste with a bad taste, I need much more water to get that rinsed out of my mouth. You actually can still do that. If you're there with the family of four, you can have access to that additional water, which is then of course with the metaphor, additional data. But then you are really using the data for the purposes. I think it's a different mindset we have to take is really thinking: “Okay. We’ve structured the data. We’ve labeled the data. We’ve pseudonymised the data. And then afterwards, we still have the data but whenever somebody wants to use it.”

Gary LaFever (Anonos)

[59:12]

I have to politely just because we have 3 minute. But I have to compliment you. We work together all the time. I've never heard that metaphor and I love it. The water, the tap, and the brushing of the teeth. So, thank you for that. Anna, would you please be the last of the panelists to answer this pivotal question?

Anna Buchta (EDPS)

[59:30]
Thank you very much for keeping me for last, which means that I have literally nothing new or original to say. But let me try. Building on some remarks of my fellow panelists, I have to say I agree with practically everything that was said. And when we speak in particular about the mindset about Data Protection by Design and by Default being baked in from the beginning in your design and your processing operations, we should really go until the end of this analysis and also ask ourselves the question: “Are the transfers really necessary? Can

I do what I need to do without transferring the data to another jurisdiction?" That goes back a little bit to what John was hinting that in the GDPR there is a high level of protection, and there is still, obviously, Chapter 5 and the commitment to a certain degree of data flows. But under conditions, which the Court now tells us have to be interpreted rather strictly.

So, at the risk of saying something not very popular, I'm afraid we should be careful not to fall into the trap of discussing here today how can we make sure that basically all the transfers that were taking place before Schrems II can continue after Schrems II as well. I don't think that this is the intended outcome. And certainly, from the point of view of the regulators, we at EDPS and others have said many times already given the fundamental constitutional importance of this ruling, there has to be a before and after Schrems II. There will have to be consequences and that, unfortunately, may mean that certain transfers will not be able to continue with the available legal instruments that we have under the GDPR and that it might, unfortunately, impact certain jurisdictions and certain types of transfers, in particular.

So, I would really like to encourage people to also have this reflection in mind when they consider their processing operations to think about transfers also consciously and consider whether they are necessary and proportionate under the circumstances and whether you really want to go down the complicated route of doing the adequacy assessment basically by yourself. Or maybe just maybe, in some cases, finding a different solution might be the easier option. I want to put in the necessary nuance. I'm not arguing here for data localisation or anything of that sort as the solution. I guess we will get to this point later anyway. Nevertheless, as I said, we need to realize that Schrems II has to have an actual impact and practice and I'm sure that this is also in this direction that the forthcoming guidance from the European regulators will go.

Gary LaFever (Anonos)

[1:03:15]

Audience Live Polling Question:

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

If you would please vote and we will show you the results of this polling in real time. And this is the first time we're using this polling, so we're hoping it works.

Okay. So, the computation is coming in. We have 700 responses already. So, for those 300 and some odd additional people, please don't be shy. No one

will know your name. And I think I really do think this is a great way to hear both from industry experts, as well as to see what your peers think.

The results of the polling are 94% of the audience that said “yes” GDPR obligations of Data Protection by Design and by Default extend beyond international data transfers? and 6% that “no.”

Panel Question No. 2:

Anna, what is your perspective on the legal principles set out in the GDPR as they relate to the three different potential “additional safeguards” – encryption, anonymisation, and Pseudonymisation. Anna, please?

Anna Buchta (EDPS)

[1:06:52]

Thank you very much. Really interesting question bringing these three topics together. I was wondering what would be the best way to go about this. And maybe if you don't mind, I would start very briefly with anonymisation just to maybe dispel some myths and set a baseline for the discussion. And, obviously, I will be happy to hear different views if there are such among the other colleagues.

So, data which is anonymised in principle is no longer personal data in the meaning of the GDPR. So, that might seem like the silver bullet that in one go solves all the problems with compliance, accountability, all the other obligations including in relation to transfers, of course. But there is a big but. There is considerable research also on the technical side that shows that true anonymisation obtaining truly anonymised data nowadays 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 that was the warning that the Working Party 29 has already expressed in its earlier guidance on Pseudonymisation techniques and anonymisation.

But that was several years ago and I think it's fair to say that the technical difficulties to truly demonstrably anonymise data may have increased since then with the increase of the volume of data that are being processed today, not to mention the element that has been hinted at, I believe, by Maggie before that anonymising data might also in many contexts reduce its usefulness for the intended purposes, and we see that also for example in the context of some scientific research users where big volumes of data there is a temptation to maybe go for full anonymisation. But quite often, in practice, that is a solution that turns out to reduce the usefulness of data. So, that might not be the preferred option.

And so, if we leave anonymisation aside, then the consequence is that the processing will fall under the GDPR because the data will still be personal and I would really like to stress this point because there have been some discussions early on in the process of negotiation of the GDPR and some misconceptions still persists. So, data that has undergone Pseudonymisation in the meaning of the GDPR remains personal data and is still subject to the requirements and the obligations on controllers that are included in the GDPR. I think that this is important to keep in mind and also indeed that the GDPR sets a certain threshold for Pseudonymisation of data, which may not necessarily correspond to the casual understanding of this term. So, this is also something where certain caution, I think, is advised.

And finally, on encryption, I believe so far in the context of possible solutions to Schrems II so to speak, encryption has been mentioned the most. But here again, I think it is fair to say that it will not be the silver bullet solution that will solve all the situations at least until such time that techniques, which actually allow to execute processing operations on encrypted data will become mainstream and not more part of experimental applications or research. So, yes, for data in storage, data in transit, under certain conditions, and in certain circumstances, encryption seems really interesting as a solution. But once again, it doesn't seem to be particularly useful if one wants to transfer data to another jurisdiction, and then perform any kind of processing operation on that data. So, I would leave it at that and look forward to the discussion.

Gary LaFever (Anonos)

[1:12:24]

Thank you very much, Anna. So, Maggie, would you please go next with your view of these three different particular approaches? Thank you.

Magali Feys (Anonos)

[1:12:32]

Thank you, Gary. Well, first of all, I want to start with saying what I think Mark and Patrick already stated that it's all about appropriate technical and organizational measures and it's an ad hoc assessment. And as said by Patrick, it really means a case by case analysis so it could well be that one of the three really suits your processing activity, or your business case, or the case where for which you want to use it. But if we then talk more global and look at the different solutions, then you can say: “Yes, encryption is good. But I think first of all, it's only one technique. It's a privacy enhancement technique. It is only one technique you're using.” So, from a data security point of view and also given I think the state of the art and the knowledge of for example,

hackers, I think we have to be very careful by just using only one technique because it's only one threshold they have to crush and they are there. Secondly, I think encryption has the single point of failure in the mere fact that it really protects data in rest. But from the moment you need your data, you have to de-encrypt it and you lose your safeguards at the same time. So, I think encryption can work but really based on which data, the risk-based approach, and a case by case analysis.

With regard to anonymisation, I think indeed as Anna pointed correctly out from a technical point of view is anonymisation today really is still something possible, for example, definitely with medical data. I truly am behind that. But finally, I think really given that with also my PhD and thinking about the potential secondary use in order to do retrospective research, you really need to have the data and today you cannot say which data you need and for which purposes. Like I said with my analogy back there with the toothbrush, but if you only get those two sips of water, it could work in some types of research or some types of processing, but you are already limiting yourself from the start. And so, I think it is then contradictory to people saying: “Well, GDPR is limiting your innovation.” Well, actually, people trying to get out of under GDPR by applying anonymisation are actually limiting themselves with regard to innovation in the future. So, I think anonymisation can really only work case by case and I don’t think in all sectors as such.

With Pseudonymisation, I have to be honest I am a big believer in the high standard of Pseudonymisation as defined in GDPR because as I said with the tap water, it decouples your data and it gives you a dataset that actually does not allow you without the additional information (the other information set) to identify the data subject. Not only by using direct identifiers but also using indirect identifiers. So, I completely agree with Anna that we see a lot of pseudonymised data where I always think people thinking failed anonymisation equals Pseudonymisation, and I don’t think that is the case under GDPR. It could be a definition of Pseudonymisation but definitely not as defined in GDPR. So, what you create is actually sort of a local anonymised dataset, but you still hold the keys, the additional information to open up that dataset whenever you need it.

We have seen that for example in hospitals where they have a lot of data. They really want to work with startups. They want to work with research projects, but they are saying: “Oh, we have no idea what to do with the data.” And it was what I was already saying. If you structured the data and if you labeled the data because there is not only GDPR in the world, I know with Schrems II we start forgetting that. But for example, there are also IP restrictions on the further use of data. There can also be contractual restrictions on what you can do with data. So, I think the labeling of data is also very important. And if you then use a GDPR-compliant Pseudonymisation tool and you pseudonymise the data and you get those

two separate datasets, then you can really start working with that data. And if you then have a case where you need the data, instead of where we used to say “Oh, just give me the data” and even in medical research we see excel sheets going forwards and backwards on emails. You say: “No.” We are now going to say: “What data do you need?” You have to make your case and only if your cases that you need more data then only the localised anonymised data. Well, we will open that data, but it shows that you have controls. You can log it as a controller. You can also establish towards the authorities what you have done with the data. You can always report back to the data subject.

So, I think in the spirit of GDPR, Pseudonymisation is really a way forward and I think that’s why it was defined as an outcome and not only as a technique. And one more thing, if you see ENISA’s Guidelines on Pseudonymisation, it actually says that you have to combine the different privacy techniques probably to achieve Pseudonymisation. So, you might have encryption, tokenization, k-anonymity. And so, you’re building a much bigger safeguard from a technical point of view. So, also from a data security point of view, I think Pseudonymisation is definitely a safeguard that is needed to be taken into consideration that’s why we also included it in our proposal of Data Embassy Principles. Thank you.

Gary LaFever (Anonos)

[1:19:01]

Thank you very much, Maggie. I think both Anna and Maggie have highlighted in order to evaluate Pseudonymisation as a potential additional safeguard, it is important to consider how it is defined within the GDPR and it's a heightened version, a very different version than what may have passed or been used in the past when using that term. So, with that, Romain, I would love to get your perspective on these three different approaches.

Romain Robert (NOYB)

[1:19:35]

No, I don't really have much to add especially to what Anna said. I totally agree with Anna, but I would even add a little thing. I think as for the question one, I'm not sure even that it is very specific to the transfer. I think security measures and encryption should already be there before any transfer because it's an obligation under the GDPR and Article 32 so it’s an obligation for security. Pseudonymisation as well is also mentioned a lot of time in the GDPR but before any transfers. Pseudonymisation is not the solution to transfers. It should be done before any transfer in a specific situation like if

you want to justify, for example, the change of purpose or if you want to evaluate the risk on the DPIAs. All these kinds of techniques are already there but before any transfers.

So, I don't think that it's an additional measure. It should be an existing measure under the GDPR and not an additional one. Regarding anonymisation, it is the same thing. If you don't need the data anymore, they should be anonymised but not just because you transferred them. So, if you don't need the data, they should be anonymised and then you are already not in the scope of the GDPR and the question of the transfer is not relevant anymore. So, that's all that I wanted to add on that. It's not really specific to the transfer in my opinion.

Gary LaFever (Anonos)

[1:20:59]

If I can, Romain, just a follow up on that because I totally agree with you. That's why the questions are structured the way they were. Data Protection by Design and by Default is not specific to transfer. The use of security and privacy tools should already be there. But the reality is, a lot of companies don't. I guess I'll put this as a question. **Would you agree that the failure to do what otherwise is required under the GDPR, almost predestine certain transfers to fail?** Whereas if you were complying with what the GDPR requires, that may put you in a position where you have a more defensible transfer.

Romain Robert (NOYB)

[1:21:44]

Yeah. Of course. But in the first place, this processing should not take place. So, of course, whether there should be a transfer is another question. In the first place, the processing should not take place. It's already not compliant. So, the transfer is another question. If you didn't encrypt the data because you had to in the first place, you should not even address the other question of transfer because they are not protected in the safe way in the EU already. So, the transfer is another question, which is going to come further. In the first place, you have to assess your security measure with encryption. You have to assess the need of Pseudonymisation if you want to change the purpose and if you want to adapt the DPIA to the risk at stake, and you have to anonymise if you don't need the data anymore. And the questions should be asked before thinking of transferring the data. That's for sure. So, it's not for any additional measures in this respect.

Gary LaFever (Anonos)

[1:22:31]

I think that's a great point and something that really has a big impact. I am a US attorney and executive, but my own view is what the GDPR brought forward is best practices that should have been done anyways. Both business purposes and out of respect for individuals, data subjects, and consumers. And so, what Schrems II really does is it shines a spotlight on the failure of doing that because now all of a sudden, a transfer is unlawful and many times it's because you weren't complying with the fundamentals anyway. So, I very much appreciate that perspective. Mark, would you please now give us your perspective on this question?

Mark Webber (Fieldfisher)

[1:23:13]

Sure. Thanks, Gary. I'm just framing this with a couple of observations to start with because I think there is a danger with some. If we are too prescriptive, we end up with prescribed localisation and maybe that's what Europe wants to achieve and maybe data transfers are going to be blocked but I hope not. I think we're here because innovation and growth has been good for society as I have said before and I think in a way Europe has backed us into a little bit of a corner around data transfers because we are now in a situation where although there is a plethora of options for data transfers for commercial businesses in the GDPR, we are really down to one - SCCs for the majority of people. Yes, there are BCRs. And yes, they are a very good tool but they are not accessible to all.

So, we were limited in what we can assess. And obviously, Schrems is making us focus on SCCs and today, but there are other potential transfer methodologies out there if we can achieve certification and if we can achieve codes of practice and maybe even get more creative. I do want to sort of have a bit of an appeal to people just to think of it laterally and where I'm going with that is these questions are fantastic. Encryption, anonymisation, Pseudonymisation - they are all things we should be thinking about, but we shouldn't be narrowing down to just these three solutions because we are going to back ourselves into another corner. I must say that because GDPR has deliberately been non-prescriptive and principle based.

When we talk about encryption, yes Article 32 mentions encryption but it talks it as appropriate and inter alia - among other things. So, it invites us to think laterally. I'm just a little bit cautious that we end up with a conclusion that it must be one of these three or you can't travel down the highway. And to that degree, if you search through the Schrems decision, no mention of any of

these three even by one word. If you go through the recent EDPB Opinion, no mention of these three because they are letting businesses make up their mind and I think it's our duty to help businesses make up their mind around what is right.

To Maggie's point, it's actually healthy to be having this discussion because we're beginning to think about what danger is involved, what we do with it, to Romain's point, whether we should be doing something with it in the first point and then how we can protect it. Then, we should look at what the options are and I think I'm just making people think about that. That's kind of a long lead into something.

Now, let's take anonymisation to start with. Yes, it removes us from the GDPR. Yes, it is difficult to do, and I think we can discount it from this conversation because if we can achieve true anonymisation, brilliant. But we can't because we use data utility to all of Maggie's points. In addition, a number of clients that we work with have a policy. There is no such thing as anonymisation in our business because frankly what's anonymised today probably isn't in 3 or 4 years' time given the advent of computing or new technologies or pairing or singling out and the rest.

So, then we are left with encryption. And I agree. Encryption is almost a prerequisite. We saw ICO enforcements just around the loss of laptops and mobile devices even pre-GDPR. If that device wasn't encrypted, they throw the book at the organization because encryption is expected. But when we do talk about encryption, we need to be careful. There's encryption at rest when something is stored and there's encryption in transit. Different types of encryption protecting against different things. There are also, you know, limitations with encryption as we're acknowledging, although there are some businesses here in Silicon Valley that are working on processing within an encrypted environment, not having to decrypt in order to do certain levels of processing, That technology, there may be some hope for us there.

So, locking things down is great. But, you know, that age old adage of you can have security without privacy, but you can't have privacy with security. So, we've got to be careful that we're not forgetting what privacy means. It's not just security. We have to want to write. We have to understand. We have to be transparent about what we're doing and there's a lot more to that. Now, if we've locked something away or take it off the internet and throw away the key, we might not be able to honor those rights because no one will get in there to respond to the Access Request or to perform the right to be forgotten requests. So, encryption can be good. It can be bad, but you've got to use it in the right proportionate way.

Then, coming onto Pseudonymisation. I think it's very powerful and businesses should be thinking about it. But there is no doubt. It's helpful

because it's a useful tool in preserving that prior identity but it has to be understood. Gary, maybe you're talking about this additional higher level of Pseudonymisation. I was looking at the ENISA paper on Pseudonymisation recently. It's fantastic, but it is very complicated and it's not all that accessible to the average layperson. So, it's part of our duty to bring Pseudonymisation to the forum to start to explain it and to start to explain that Pseudonymisation isn't a thing. It's a technique and there are different ways of doing it. And then when you perform that Pseudonymisation, it can be strong Pseudonymisation or it can be a relatively weak Pseudonymisation. And then, you introduce these extra concepts of the identity must be in the hands of the controller. So, explaining how that works and how that breaks down and then not losing sight of how that pseudonymised information is then used because it's often then used alongside other identifiers or identified information and then we get into risk of linkability. We get in risk of inference, the ability to push back, and reverse the Pseudonymisation.

I don't think there is enough supporting evidence for businesses to work out how to use Pseudonymisation well, but I think it can be used well. But I also see situations where it can be limiting because ultimately do I want to use pseudonyms in the States when I'm trying to email my colleague? No. I need to know their name. I need to know some of that raw data. So, having businesses explain how those limitations can be overcome and explain techniques to deploy Pseudonymisation could be really helpful. But I do fear prescription and I fear prescription because what we think is good today in the light of one decision isn't necessarily where we want to be in 2 years or in 3 years.

I sit here in Silicon Valley looking at technologies, working on AI/ML projects. We are almost at the forefront of some of the things that are coming through but we're always looking back at law and think if only we've thought of the biggest barrier to innovation at the moment is ePrivacy because ePrivacy reflects a position and a state mind in 2002 and small adjustments as a result of telecom reform in 2009. That became descriptive, tried to be technology neutral, and restricts quite a lot now. Let's not do the same when we legislate and give guidance and let's remember those clauses, which they as appropriate, which may include inter alia. Let's remember guidance is guidance and we can think beyond that guidance when we see it from EDPB and work within the parameters that we're given. So, hope that gives you a bit of a steer in where I'm coming from.

Gary LaFever (Anonos)

[1:31:18]

Thank you, Mark. Absolutely. Patrick, please, if you could add your perspective?

Patrick Van Eecke (Cooley)

[1:31:23]

Sure. And I think it's already clear from the discussion that there is no one size fits all solution. But for sure, in certain circumstances for some scenarios, anonymisation, encryption, and Pseudonymisation could certainly serve the purpose and I just wanted to elaborate a little bit further on what the predecessors actually have been working on or making statements on. And it is, we heard that if you've got anonymous data, that it's not personal data. You're out of scope of the GDPR. You're out of scope of the Chapter 5 of the GDPR on data transfers. So, anonymous data, you can actually transfer to anywhere in the world because it's anonymous.

Now, we know from Anna, that she has some doubts on full anonymisation. And yes, of course, we need to make sure that from a technical perspective, you do need to take into account the necessary measures to truly anonymise. But still when you go back to the GDPR and you can actually make a comparison between the current GDPR and the Data Protection Directive, the Data Protection Directive talking about anonymisation, it was really kind of a binary kind of thing. Yes, it's anonymous or it's not. But if you look now, in the GDPR Recital 26. I don't want to become too technical. But if you go and look at Recital 26, these are two such important words, it says reasonably likely to be used. This is not binary. This means that all the means reasonably likely to be used to identify an individual. Well, then, of course, then it is not anonymous data. But it's not binary. And then, the Recital continues and mainly it says we need to take into account costs, amount of time required for identification, etc. So, having said that, anonymisation could maybe lead to making a statement that it's not personal data.

But actually, I want to take it one step further, namely Pseudonymisation. We all agree that Pseudonymisation as such is not anonymisation. It's not anonymous data. But if you put that discussion in the context of data transfers where you pseudonymise on EU territory the data, you keep the key, you transfer the data overseas to another country where they don't have access to the data, the country considers that the data over there are anonymous data. From a contextual perspective, yes because there are no means reasonably likely to be used to de-identify those data. If we would be able to make that statement, that means there is no Chapter 5 that should be applicable because there is no data transfer. Of course, this is something still waiting for the EDPB to come up with such kind of a bold statement. But this would be in certain scenarios it could be a solution, and I know Romain you probably wouldn't say yes and that's not safe, etc. But actually, at the end, the 63 pages of the Court of Justice decision, what is it about? Well, it's about as a company transferring data outside of Europe, can you assure that surveillance authorities do not have the possibility to read the personal data

on your system? So, if you're having to pseudonymise and the controller has the key based in the European Union, you could claim that technically, indeed, that is not possible. So, I just want to put it on the table because I do know this is a topic that you can go in different directions to. But still, I do believe that this kind of hot potato is something that the EDPB should be discussing and should come up with a kind of what's the way forward on that.

Gary LaFever (Anonos)

[1:35:41]

Great perspective, Patrick. I know because I helped co-author the memo with Maggie that the memo to the EDPB on Data Embassy Principles was just that concept that if the data exporter keeps the keys and they have to show technologically that they're the only ones who can do it. And I do want to share a screen very quickly. There's been several references to the ENISA Guidelines. And we would encourage you, if you go to ENISAGuidelines.com, it walks through those. They are an approach to do exactly what Patrick just described, which is to ensure technologically statistically from a data science perspective that the recipient of the pseudonymized data is not able to re-link to identity, and whether or not that would be considered anonymous for purposes of the GDPR. Mark had a question for Patrick. Mark, if you want to raise that?

Mark Webber (Fieldfisher)

[1:36:42]

It's a thought. It's not necessarily for Patrick. Again, one of the things we need to be careful again to fall into the trap of is assuming that the controller is always in the EU because keeping a key in the EU is fine, but there are many controllers and many users of data by controllers outside of the EU into the countries. As much as anything, it's an observation that if they're the controller, they naturally have the ability to callback that Pseudonymisation and then they're in the US, they're in China, they're in India or wherever they are and just to sort of float in that as an additional concept and also a caution to everybody thinking about it. It's not always binary, right? Controller to controller to controller examples are out there, and we can't assume that data is always and can always be in the EU.

In fact, extraterritoriality provisions of the GDPR do just that. Article 3 was designed to make sure they exported the GDPR to processes that were targeting and monitoring behavior. And so, Article 3(2) already exports the GDPR. I think what we are dealing here with Schrems is looking at exporting the Charter as well to all of those organizations and seeing that compliance

and that's one of the things we're struggling with. So, I feel for businesses that aren't in that binary scenario because even when we see guidance, they are going to be very focused on the A to B, not the A to A to B to C to D that most of us live in in our real world.

Gary LaFever (Anonos)

[1:38:30]

Thank you, Mark. John, if you wouldn't mind wrapping up with your response to this question. If you could kind of incorporate part of what Mark and Patrick said, which is with regard to these different techniques and if you could, focusing on Pseudonymisation if, in fact, you have satisfied the requirements of the GDPR so they can only be relinked with access to the additional information, we'll keep that the keys. The importance of those keys being only in an EU country, and not accessible by co-controllers or otherwise. If you would, John?

John Bowman (Promontory)

[1:39:06]

Thanks, Gary. So, maybe just to take a step back. One of the key points, which I think Mark raised, is that we don't know what technology is coming along. I did a little diagram, which I must admit was inspired by a visual representation of a conference back in Berlin a few years ago, which shows regulation and technology. So, as time goes on, effectively the gap sort of increases between the two. So, to what extent can regulation keep up with technology? We can argue that at least GDPR is a principles-based regulation, which cites examples of encryption and Pseudonymisation as data protection or privacy enhancing measures. So, I think it's important to bear that in mind and all those Pseudonymisation and encryption might be the latest and greatest, but something else either might come along which is better or some other measure might come along, which is able to unpick these current solutions.

Having said that, I think data controllers and data exporters in particular need to think about what are the outcomes? And really what is the safety of access to the keys as you described in Pseudonymisation context and the actual sort of data which are being transferred possibly for research purposes or for some other purpose which the recipient requires it for. I think it's a difficult question to answer in that every sort of scenario is going to be different. But really, any data controller or any data exporter needs to look at the sort of menu of

measures which are available to them and consider them in the context of the processing that they're doing. So, life sciences or a pharmaceutical company in particular might well consider that it's important to share the results or the data of their research to other laboratories around the world. COVID, in some ways, is bringing this to the fore with all the research and so on. And there might be benefits to humankind in terms of that data being accessible because it's a global problem, let's face it.

But really, they need to think about what the safeguards are in place. And if it's EU subject data, it may well be a sensible approach. I'm not advising that this approach is taken, but it certainly may well be sensible to think about the secure environment that the keys to pseudonymise data are kept in. And if that means looking at it in terms of the EU, then that's certainly an option, which should be considered. Again, just another more general point is every organization that is subject to the GDPR has to do a ROPA - the record of processing activities. So, before you even think about transferring the data, you got to know what your data processing activities are, sensitivity of the data, the legal basis that you base that processing upon, and if it's transferred out of the EU to a third country without an adequacy decision, what measures do you put in place.

So, of course, this comes back to the Schrems question, enhanced and supplementary measures, which are based on SCC transfers and those could be technical and organizational measures. Obviously, we're still awaiting the guidance from the EDPB, which of course will be incredibly helpful when it comes. But, in the meantime, do everything that you can to protect that data in transit and ensure that the recipient has the appropriate safeguards in place. So, that's the way I'd sort of wrap up that question.

Gary LaFever (Anonos)

[1:43:25]

Fantastic. Thank you very much. And I have to admit, in fact, it's not much of a contest, John, you win for the most creative props so thank you for that.

John Bowman (Promontory)

[1:43:36]

I'll try and confirm that Pseudonymisation doesn't appear in this toy-sized miniature copy of the Charter of Fundamental Rights. They probably couldn't fit the word onto one page.

Gary LaFever (Anonos)

[1:43:46]

That's great. So, you can tell the level of discourse and discussion we've had here that this is something that's very relevant to everyone. We are not going to have the opportunity to get to the 700+ questions that have been submitted. So, we actually have taken the liberty of starting a LinkedIn Group, and I would invite all of you as you are sitting at your monitor right now to actually go into LinkedIn and just type in “Schrems II - Lawful Transfer”. We want to continue this discourse and dialogue. We think it is critical. Obviously, as the actual Opinion comes out, the updated SCCs from the Commission, the EDPBs Opinion, there are going to be a lot of things that we can interact on. So, we would encourage all of those with interest to join this LinkedIn Working Group so we can continue this discussion beyond this webinar. So, again, “Schrems II - Lawful Data Transfer” in LinkedIn.

Panel Question No. 3:

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

Anna, please?

Anna Buchta (EDPS)

[1:46:00]

Thank you. Well, I would say that it might well be quite a realistic scenario in some cases, during the negotiations of the GDPR and John may remember that the example of a bakery on the corner was very often used as your typical data controller. So, I would guess that they may have the possibility to still maintain a customer's list without considering transfers necessarily. But I guess that this is not the kind of scenario you're hinting at with your question.

So, as I said before, in our supervisory practice at EDPS already before Schrems II, we have identified and we have spoken about situations, types of data, types of processing that in our view should not be transferred out of the EU or out of the EEA. So, I think this still stands for us. 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. Compliance with EU rules and we are committed to working with our partners in the EDPB towards such understanding and interpretation of the rules of transfers and implications of Schrems II that would still open or leave a possibility for transfers to as many

jurisdictions as possible provided of course that compliance with the Court judgment can be ensured.

Gary LaFever (Anonos)

[1:47:52]

Thank you. Very well put. Romain, would you please go next with your answer to that question?

Romain Robert (NOYB)

[1:47:59]

Sure. Again, I fully agree with Anna and I'm very happy to see what the EDPS already stated like a couple of days ago and especially with their paper on the use of Microsoft within the EU institution in July when EDPS already stated a lot of issues and problems with the use of Microsoft especially Microsoft 365 where there is no possibility to use Microsoft 365 without any transfer to the US. It has been confirmed really recently by the German Conference of the DPAs that it has been raised 2 years ago by the Dutch DPA and by the Dutch Government regarding the use of Microsoft products by the Dutch Authorities. So, that's a nice example and I think the DPA has really pointed out really rightly what was wrong with the reading and interpretation of the transfer rule regarding the use of other products like Facebook and Google for example. I think Microsoft is a super nice example as well.

And as far as I remember in the EDPS statement in the paper in July, EDPS also pointed out the data location principle, which was encouraged by the EDPS but not suggested as a rule and I totally agree with them. It's a nice way to go. It's not a solution but I think it should be also a nice way to go in the first place to wonder whether the transfer is necessary or not beforehand. Just to mention that NOYB is also working on this case as well. So, on the use of other products than Google and Facebook transferring data to the US.

On localisation, there is also another issue that is sometimes mentioned is of course what about US companies based in the EU might be subjected to the FISA Court? Nobody has the solution and the answer to this question. So, is Microsoft subject to FISA even when Microsoft is based in the EU? We don't even know. There is no clear answer to that. To answer this as well, that the Court of Justice Schrems II in my opinion and I want to be a little bit provocative with this respect, it's not about the transfer of data outside of the EU. Schrems II is about the use of SCCs by a US-based company called Facebook in the first place. That is what Schrems II is about, and it has ended up not very well for the Privacy Shield that's true. But in the first place, nobody

asked, especially not NOYB, to challenge the Privacy Shield. In the first place, Schrems II is about transfer by Facebook of data outside of the EU to the US based on the SCC and not about the general principle of transfer outside of the EU.

So, I don't think that the court just made a general statement about the adequacy decision in other third countries. The Court addressed the specific situation of the US raising two main arguments why the US law was not complying with the Charter of Fundamental Rights of the EU first with massive surveillance and bulk collection of data and second with regard to judicial redress, which is also a question which is not addressed that often. 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 and it has to be granted and provided to the citizen or to the holder of the rights in the EU? How do you create a judicial redress with contractual clauses? You cannot create a judicial avenue to citizens with a contract that you signed between two entities to my knowledge. I guess you cannot change the US law just by signing a contract between a controller in the EU and a controller or processor in the US. So, that's another problem that is raised by the Max Schrems II decision in my opinion.

So, basically, what about US companies that might be subject to FISA? My knowledge of US law is not enough to understand or to have a final conclusion about this question. And the second question is of course not restrictive but a very delineated scope of the question addressed by the Court. This question in Schrems II was about the transfer of Facebook data based on the SCCs. So, we should not make too broad an interpretation of the Schrems II decision as well. I mean, it doesn't mean that it does not raise questions for other companies like Facebook of course. That's not what I say, but let's try to go piece by piece and try in the first place to understand what the Court meant in this specific case and try to understand what it meant in the other cases as well.

What I want to avoid is also to go for Schrems III, and I totally agree with Anna again that we had 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. It's not a surprise. The Court already re-affirmed what they said 5 years ago. Do we want to go back to look for another? I think the judge will be a little bit disturbed. They have other things to do than confirming again and again and again what they already said in the past. I think that they would like to do something else. They have the right to variety as well of legal issues. So, I think we have to listen to the Court this time and try to avoid reproducing and doing the same mistake again.

Gary LaFever (Anonos)

[1:53:14]

Thank you. John, can we get your perspective then please?

John Bowman (Promontory)

[1:53:19]

Okay. I think data localisation is a matter for those businesses who have international footprints. Again, understanding their data flows, where the information is going, what the safeguards that are in place particularly at the recipient's end - those are important elements. But clearly, Privacy Shield under the Schrems II judgment 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 organizations can start thinking about what those are whether they're technical organizations or principles based measures. And obviously, we await the guidance.

So, hopefully, once the guidance is clear, then the companies can work out what's the best for them. But really, to some extent, it may be obvious to some companies or to many organizations that some countries present a greater risk than others. And that has to be all part of the assessment. But also in that context, the actual sort of sensitivity of the data and what the outcomes and potential harms to individual data subjects must also be considered. But there's a lot of points to be taken on board there. But whether that results in a data localisation sort of approach really depends on sort of weighing up the risks and the benefits and the measures and safeguards in place. But, clearly, SCCs did survive the Schrems II decision, but with those additional measures and considerations, which needs to be taken into place and our advice would be companies should take those measures seriously and really think about what they're doing.

Gary LaFever (Anonos)

[1:55:23]

Thank you, John. Patrick, if you would, please?

Patrick Van Eecke (Cooley)

[1:55:26]

In just 30 seconds. So, for sure, I do believe that localisation or relocation should be part of the exercise. It's part of the menu of the different measures that organizations should be taking into account. Next to the technological measures, this is kind of an organizational measure thinking about for the past few years, we've been storing our data on the server in that country. But why do we do that? Maybe we can also do it somewhere else? The only concern I'm having is that localisation could lead to balkinization, and I'm really concerned about that, because I'm not concerned indeed about the bakery shop. But I'm concerned about global businesses where, for example, you've got an HR Director who's responsible and who has EMEA responsibilities - Europe, Middle East, Africa. And today, maybe that HR Director is based in Dubai, but maybe in 2 years, another HR Director would have that function based in Australia. These are 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. So, companies have always got to be confronted with the need for transferring personal data. So, I do believe localisation should be part of the exercise. It's also part of the strategy or the methodology we have at Cooley, the Maori methodology. The R of Maori stands for Relocation and very happy to discuss that whenever we would have more time to do that.

Gary LaFever (Anonos)

[1:57:02]

Fantastic. Thank you very much. So, I wanted everyone to know that in the last few minutes, we've had over 400 people sign up for the LinkedIn Working Group. So, again, we would encourage those who haven't to do so and to tell your colleagues because we have not had a chance to touch on many of the questions you have submitted.

Panel Question No. 4:

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

Magali Feys (Anonos)

[1:57:46]

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.

So, I think not today. But on the other hand, I disagree a little bit with Romain. We live in a world today where people have to do business and we have to be able to send emails to each other. So, we have our work cut out for all of us.

Gary LaFever (Anonos)

[1:58:35]

Romain, would you please answer this last question. Cloud providers are saying: “Everything's okay. We have SCCs in place.” What is an EU company wanting to use a US cloud, SaaS, or outsourcing company? What is your view on their ability to solely rely on those assertions?

Romain Robert (NOYB)

[1:58:54]

In this respect, I would like to refer to the “Next Steps for EU companies & FAQs” available on the NOYB website. I don't know if you've seen them. But I think it was also useful because we had a lot of positive comments and feedback. We are also trying to help the businesses to cope with the judgment. We don’t have the solution. We are just part of the problem for sure. But we try to be a part of the solution as well. I think the question that was suggested to the SMEs in the EU and of course with the other companies to ask to the providers were also really useful because we had quite a couple of nice answers. You would also see on our website that we published the answers of some companies. They still don’t even seem to try to make an effort, and I think it’s also the message.

You see that some people are struggling, and I really feel for them but I don’t have really much empathy for companies who don’t even provide an answer to the question. So, that means that they’re not going to try to find a solution. At least to say they’re relying on SCCs or they try to find additional measures would be a nice start. But you couldn’t see this kind of solution from a lot of companies. They did not provide any solutions. They did not work on the subject, and I think it’s not a sign of good faith.

And on a final note, I would like to also mention that we at NOYB are working as well on this anonymisation and Pseudonymisation techniques. We are working on cases where we will probably challenge this alleged anonymisation of companies transferring the data out of the EU. So, I hope that we are going to have a clear answer from the Court and from maybe the ECJ on this kind of question because we really think that is a crucial question. In this respect, if anonymisation and Pseudonymisation as presented by this

company are real Pseudonymisation and real anonymisation under the GDPR and whether it can it be relied upon to transfer the data outside of the EU. So, we are working on this as well.

Gary LaFever (Anonos)

[2:00:44]

That's a great perspective and I think it highlights that terminology is important and that imprecise use of terms can be used to try to hide improper use of technology or data.

Anna, would you mind? In respect of everyone's time, you will be the last panelist to answer this question. You get to bring this home and make the webinar the great success we hope it is.

Anna Buchta (EDPS)

[2:01:29]

Anyway, as I said before, I think what I take away from every webinar that I have attended in the past weeks are the very high expectations towards the regulators to provide very clear, harmonized, practical, bullet proof, court proof Guidance by next week. So, I think I would like to use this opportunity to maybe also stress that obviously as regulators, we are very much aware of the difficult predicament most businesses are finding themselves in. And there is really a lot of hard work going into providing this Guidance as soon as possible. At the same time, I think I would encourage people to have realistic expectations, both regarding the timeline, because there is also another process that is taking place right now and this is the update by the European Commission of the existing SCCs that has been announced already some time since the GDPR actually.

But now, apparently, we are entering the finishing line and there are obvious interconnections and interdependencies between any guidance both Schrems and supplementary measures and what the new SCCs will look like. So, it's also crucial that these two processes are aligned. But the preparation of the SCCs on the Commission side apparently is taking slightly more time than expected. And so, we have not seen any drafts yet. That might have an impact on the one hand on the timing. And at the same time, it may also be that this initial Guidance may not necessarily offer all the answers because unfortunately the Court ruling is not very explicit as to what kind of supplementary measures might be appropriate for what jurisdiction.

So, what I'm trying to say is that regulators can only do what they can do and it may not necessarily live up to all the very high expectations that I also

gathered from some of the questions that might be out there. So, be patient. Please be patient. Wait for it. We are doing our best. But that will not remove the baseline of the GDPR principles, and this is accountability, which means that every controller has to take steps by themselves and apply measures which are necessary to ensure compliance with the GDPR including the provisions on transfers. Thank you.

Gary LaFever (Anonos)

[2:04:18]

Thank you, Anna. I think it's a great way for us to end and I just want to highlight again over 2300 people signed up for this webinar in less than 4 days. This is a reflection of the importance of this issue, and I think you've heard from all the panelists that this issue is not just about data protection for data protection's sake and it's not just about allowing companies to do what they've done in the past so they can continue to make profits. Rather, it's a way of having controlled, managed innovation that can meet everyone's need to have lawful enablement and innovation.

And it has been a pleasure on behalf of Anonos to sponsor this event and we welcome anyone to reach out to us. Our view with 8 years of R&D is that you can actually deliver Data Liquidity and what we mean by that is universal data protection that takes all these issues of lawfulness, data science, data engineering, and utility. If you have any questions regarding that, please reach out to anonos.com. But most importantly, please think of joining the LinkedIn Working Group so we can continue this dialogue because as the SCCs come out from the European Commission and as the Guidance comes out from the EDPB, it will be professionals such as those that have been so kind to give their time and beyond the panel and those of you in the audience that can make this work for all of us. So, thank you very much on behalf of the panelists and on behalf of Anonos. It has been a pleasure and an honor. Thank you very much.

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.