Podcast

Crossing Borders: Navigating the EU's New Standard Contractual Clauses

By Mary T. Costigan

February 16, 2022

Meet the Authors

Mary T. Costigan

Principal

908-795-5135

Mary.Costigan@jacksonlewis.com

Related Services

International Employment

Privacy, Data and Cybersecurity

Technology

Details

February 16, 2022

The EU Commission has published new Standard Contractual Clauses to facilitate transfers of personal data from the EU to countries lacking an EU adequacy decision, including the U.S.

Jackson Lewis P.C. · Crossing Borders: Navigating the EU's new Standard Contractual Clauses

Listen on Apple Podcasts

Listen on libsyn

Listen on Google Podcasts

Listen on pandora

Listen on Soundcloud

Listen on Spotify

YouTube

Listen on STITCHER

Takeaways

Crossing Borders: Navigating the EU's New Standard Contractual Clauses

The EU Commission has published new Standard Contractual Clauses to facilitate transfers of personal data from the EU to countries lacking an EU adequacy decision, including the U.S.

What Employers Need to Know

- Transferring personal data from the EU or U.K. to the U.S. or permitting access to personal data in the EU or U.K. from the U.S., is a cross-border transfer that must comply with the GDPR.
- In certain circumstances, the GDPR requires the data exporter to use an "adequate transfer mechanism" to facilitate the transfer.
- Standard contractual clauses or model clauses are one such mechanism.
- The EU Commission recently published updated model clauses to replace the existing templates.
- These new clauses require the data exporter and importer to conduct a documented transfer impact assessment (TIA) to ensure the transferred data receives an adequate level of protection.
- The TIA should include an assessment of whether U.S. surveillance laws may impact the transferred data.

- In the event the TIA concludes the clauses do not provide adequate protection, the parties must provide additional safeguards to protect the data.
- The U.K. has drafted similar updated clauses that will be published in the near future. These clauses will also require the parties to conduct a TIA.

Transcript

Alitia (00:06):

Welcome to Jackson Lewis' podcast, We get work™. Focused solely on workplace issues everywhere, and under any circumstances, it is our job to help employers develop proactive strategies, strong policies, and business-oriented solutions to cultivate a workforce that is engaged, stable, and diverse. Our podcast identifies the issues dominating the workplace in its continuing evolution, and helps answer the question on every employer's mind: How will my business be impacted?

The EU commission has published new standard contractual clauses to facilitate transfers of personal data from the EU to countries lacking an EU adequacy decision, including the United States. On this episode of We get work™, we discuss these new clauses and how they could apply to various cross-border transfer scenarios, including the transfer of human resource data in the technology industry.

Our hosts today are Mary Costigan, Of Counsel in the Berkeley Heights office of Jackson Lewis, and Beverley Flynn, head of data protection, and partner at UK firm Stevens & Bolton. Mary advises employers on data privacy and cyber security issues, best practices, and preventative safeguards for a wide array of data protection laws.

Beverley has over 25 years of experience working in house, including as a data protection officer, and providing in-house data protection and privacy support at a major multinational company. After a meeting at a global summit of the International Association of Privacy Professionals, the two women family had much in common professionally, and a shared passion for advising clients on critical privacy issues.

Mary and Beverley, the question on everyone's mind today is, how do technology companies prepare for the EU commission's new standard contractual clauses, and how does that impact my business?

Mary (02:04):

Beverley, it's great to have a chance to catch up with you again and discuss what's happening in the world of data protection. So, thanks for joining us.

So, as Alicia said today, we're talking about the GDPR and cross-border transfers of data. We both have clients that transfer data, personal data, from the EU to the US. Sometimes it's employee data, in other cases it's consumer or client data, and we also have clients that access personal data in the EU from the US.

These transfers are known as cross-border transfers, and under the GDPR, the parties to the transfer must use what's called an adequate transfer mechanism to facilitate the transfer.

So, Beverley, I know you work extensively with clients that conduct these types of

transfers. What is an adequate transfer mechanism, and why is it required to transfer personal data to the US?

Beverley (02:51):

Well, hi, Mary, and many thanks for having me. I think it's really important to understand that in the UK and the EU, we've had personal data protection laws stemming back to the 1980s, and the GDPR is actually the third iteration of those laws protecting personal data. And the GDPR provides a framework of rules applicable to the processing and use of that personal data. And in particular, it's transferred to third countries.

There are now two separate regimes following Brexit, which is the UK's exit from the EU. So, not only do we have to contend with the EU GDPR, we also have to contend with the UK GDPR. One of the rules of each of these is to prohibit the transfer of personal data to a third party in a third country, unless there is actual adequate protection for the rights and freedoms of individuals in place.

And that's where we get the GDPR adequate transfer mechanism. In order to meet the adequacy requirements, different adequacy mechanisms have been put in place. For example, in the past, we had the Safe Harbor and Privacy Shield in the case of transfers to the US, which are now defunct. And we also use the standard contractual clauses, the SCCs, or the model clauses, which I'll come on to talk about in more detail.

In the past, or sometimes for intergroup transfers, you can also use binding corporate rules. But actually, to answer your question, a GDPR adequate transfer mechanism that most entities use is the use of the SCCs, the standard contractual clauses.

Mary (04:27):

So, Beverley, here in the US, we don't have an omnibus data protection law like the GDPR. Instead, we have a growing patchwork of data protection laws at both the state and federal level. In fact, I recently heard that the US has two-thirds of the world's data protection laws, which can definitely make compliance challenging. And each of these laws has its own definition of personal information, so we have to be mindful of that definition. How does the GDPR define personal data for the purposes of a cross-border transfer?

Beverley (04:57):

Good point. Yes. It's probably first worth understanding briefly what we mean by personal data, as I sense it's a wider term than one that is readily understood in the US. So, for context, when we talk about the GDPR, we're talking about two things: the processing, and the processing of personal data. And by personal data, we mean any information relating as an identifier to an identifiable natural person.

So, for example, it can be something such as a name, an identification number, location data, an online identifier, or even specific factors such as physical, genetic, mental, economic, cultural, or social identity. So, it doesn't apply to anyone who has passed away, because they have to be an identifiable living person. But it can include

business/email addresses, because they contain a name, or it can include an IP address, or an employee roll number, a national insurance number, car number plate, and VIN number, even, as well as such information as name, address, or date of birth.

And if you take an employee, for example, it goes wider than their name, but can actually include their personal emails, data in work emails which is about them, such as appraisals, financial information, or family or health data. And it's this health data or mental health data which under the GDPR is known as special or sensitive data. And that has special, even more, protection than the usual personal data.

When we talk about processing, it's again a widely interpreted term, so it can simply apply to holding, accessing, or deleting the personal data, which counts. So, for example, if personal data is held on a server, or a third party is used to host the data, or you include IT support or payroll, as well as the usual HR activists, those are all known as processing personal data.

And finally, Mary, I don't really want to scare your listeners, but just to mention, it not only encompasses personal data held on computer, or in paper files, but extends to other formats in which personal data is processed. So, for example, if you have video footage, you have CCTV in your building, or your car park, there are telephone recordings, telephone messages, Zoom chats, WhatsApp chats, Teams chats, texts, et cetera, they all count towards personal data being processed. So, it's pretty extensive.

Mary (07:41):

That's actually a very helpful reminder because many US data protection laws apply only to computerized data. So, that's something we're not used to focusing on and factoring in.

Beverley, you mentioned earlier that the EU-US Privacy Shield, until recently, was one of the transfer mechanisms US organizations relied upon. Just to give our listeners a little context, in mid-2020, the court of justice of the European Union struck down the Privacy Shield in a decision widely known as Schrems II.

In a nutshell, the court found that the Privacy Shield Framework did not ensure that the personal data transferred to the US from the EU received a level of protection that was considered essentially equivalent to that that it would receive under EU data protection law.

The interesting part of that decision is the court focused on US surveillance laws and the risk they posed to the transferred data. So, as a result of this Privacy Shield Framework being invalidated, many of the organizations in the US are now using standard contractual clauses or the model clauses as the mechanism for transferring personal data to the US.

So, here in the US, we do have data sharing agreements and business associate agreements, but we don't have a mechanism for transferring data quite like the standard contractual clauses. How would you explain these clauses and their purpose?

Beverley (09:02):

Well, Mary, that's a good question. Following Schrems II, there was a wholesale shift on data transfers from the EU and the UK to the US being undertaken via standard contractual clauses. And of course, the EU has just introduced new standard contractual clauses.

And what the clauses do is, they mean that the parties can record, in contractual terms, the basis of the transfer with a view to giving adequate protection to the individuals, the data subjects. Now, the clauses cannot be amended commercially, so they have to be retained in their standard format. And there is a lot of information which needs to be added. Technical organizational measures, details of the companies that are being transferred to, details of subcontractors and subprocesses.

And you mentioned Schrems II. And in light of Schrems II, the new EU model clauses do give a nod to Schrems II, and you have to look at whether or not the country that you are transferring to can meet the Schrems II requirements and provide sufficient safeguards.

Mary (10:18):

So, when we're talking about these model clauses or the standard contractual clauses, we're really talking about standardized contract templates that have been issued by the EU commission. I know the original clauses date back to 2004, and you just referenced the new clauses, which the EU commission issued this past summer, so we now have a new set of model clause templates. Are there any significant changes with these new templates?

Beverley (10:44):

Yes, Mary. You are right. They are very different. And what they do in particular is they cater for new scenarios, which is very much welcome. Those who are aware of the original clauses will recall that they only dealt with very limited situations. So, controller-to-controller transfers, and so-called controller-to-processor transfers.

In recent years, the business organizations found that very restrictive, and the new EU SCCs are modal. That means that they address more scenarios than before. And in particular, they cover the transfer of personal data from a processor to another processor, or indeed the scenario where you've got a processor who is transferring data back to the controller. These were never covered by the earlier clauses, and did give us some difficulties.

In addition, the EDPB has issued guidance on how to reassess the position in light of Schrems II that I mentioned. And they do give a nod to a transfer impact assessment, or enable you to think about the Schrems II position, which is really useful.

I should mention that the UK transfers to the US cannot currently rely on the new EU standard clauses because of Brexit, I'm afraid. So, if you are transferring from the EU or from the UK, you may have to use both the original clauses for the UK and the new EU clauses for transfers from the EU.

Another thing to bear in mind is that the UK has just issued a new law dealing with transfers to third countries. So, we may be that, in due course, rather than using the

old model clauses, you'll have to use an internet national data transfer agreement, or more simply, an addendum to apply to the new EU SCCs. So, watch his face. It will probably come into force around 21st of March, 2022, unless the UK parliament raises objections. I appreciate it's complicated, but that's because we've got the UK and the EU to consider.

I mentioned the transfer impact assessment, Mary, that the EDPB has suggested that businesses undertake when they're transferring to third countries, and the model clauses do give a nod to that. When you're transferring to the US now, how are the US national surveillance laws that may affect the US data importer's ability, and essentially affect the equivalent level of protection? Have you got any ideas on how the organizations will need to conduct these analyses?

Mary (13:28):

That's a great question, Beverley, and it's causing quite a bit of confusion with US companies. There's currently no standard assessment tool for conducting a TIA, at least under the EU GDPR. And while both the EU data exporter and the US data importer are responsible for conducting this assessment, and also for warranting that they have no reason to believe the US laws will prevent the importer from complying with the SCCs, the burden really is on the US data importer to make this determination.

This involves reviewing several factors, which could include the potential threat to the security and privacy of the transferred data, the nature and the sensitivity of the transferred data, any relevant data protection laws in the US regulations or standards that might apply to this data, the rights of law enforcement agencies or US intelligence services to access the transferred data, and also any opportunities for EU data subjects to seek redress for any violations or alleged violations of their privacy rights in the US.

So, assessing the potential impact of the US surveillance laws is perhaps the hardest part of this analysis, and that's where US companies are struggling most. In the Schrems II decision, the court focused on two issues here. Section 702 of the Foreign Intelligence Surveillance Act, also known as FISA 702, and they also focused on Executive Order 12333. So, since the court called out these two, well, this executive order and this federal law, many of the transfer impact assessments we're seeing now include questions asking the data importer to disclose whether it's subject defies a 702 or the executive order, and also to disclose whether it's received a request from an intelligence agency in the past.

So, just briefly, FISA 702 is a federal statute that regulates electronic surveillance conducted for national security or foreign intelligence purposes in the US. Under FISA 702, the government requests court authorization to issue an order requiring an electronic communication service provider in the US to provide the government with all information, facilities, or assistance that it needs to conduct the surveillance.

Executive Order 1233 is not a law. This is a general directive that authorizes US national intelligence agencies to surveillance outside the US. The executive order doesn't include any authorization to compel private companies to disclose data.

With this in mind, in response to the court's Schrems II decision, the US department of commerce published a white paper in September of 2020. And the white paper addresses the court's concerns about the potential impact of the surveillance on the privacy and security of data transferred to the US. So, the white paper's not legal advice, but it's very helpful as a starting point for data importers when they're conducting a transfer impact assessment.

Just briefly, the paper makes four noteworthy points. First, most US companies do not handle data that would be of interest to US intelligence agencies.

Second, US companies whose EU operations involve ordinary commercial products or services, and whose transfers of personal data involve ordinary commercial information, such as employee, customer or sales records, would have no basis to believe US intelligence agencies would seek to collect that data.

Third, the overwhelming majority of US companies are not electronic communication service providers who would be subject to FISA 702, and the overwhelming majority have never received orders to disclose data under FISA 702, or have never provided personal data to US intelligence agencies.

Finally, fourth, several US statutes provide individuals of any nationality with an opportunity to seek redress in US courts for an alleged violation of FISA 702.

After conducting this assessment, keeping those considerations in mind, in the event the data importer concludes it may be subject to US surveillance, and the standard contractual clauses don't provide an essential equivalent of protection, then it should consider incorporating supplemental safeguards into the model clauses.

For example, this could mean specifically warranting that it will not voluntarily assist the government in conducting operations under the executive order. It could mean warranting that it will implement strong encryption to defeat potential interception of the data when it's in transit, or warrant that it is not an electronic communications service provider, and also warranting that it will fight any 702 directive.

So, that's a quick summary of a complicated issue, but hopefully it provides some insight on how US companies can address the transfer impact assessment, and in particular, the US surveillance questions.

Beverley (18:27):

Thank you, Mary. I mean, they don't make it easy, really. Not only do we have two sets of model clauses that need to cater for every scenario, we also have to undertake the transfer impact assessment, and rely on advice from the local lawyers. So, it is quite a large task, actually, when you think about it.

Mary (18:46):

So, Beverley, when do organizations need to start using the new model clause templates for transferring data to the US?

Beverley (18:52):

Well, it's complicated in light of Brexit, but from the EU perspective, straight away for new contracts and for existing contracts that are already in place, they need to start replacing them as they will no longer be valid from 27th of December to 2022. We, which is not actually that far away I should add. The position is slightly different for transfers from the UK to the US, but really bear in mind, if you are transferring from the EU to the US 27 December, 2022, your old SCCs need to have been replaced by then.

So, Mary, just looking at the SCCs, are there any steps you'd recommend that US organizations take now to prepare or implement the new SCCs?

Mary (19:40):

There definitely are several steps. First of all, it's most important to understand when a transfer takes place. So, transfer is not only the transfer in the traditional sense, where you're sending data from the EU to the US, but it's also when you allow an individual or an organization in the US to access data while it's stored, perhaps in a server in the EU. So, that's an important fact to keep in mind.

Second, it's helpful to know what data is in scope. So, is this customer data? Is it employee data? Is it highly sensitive data, special category data? Knowing this will help drive your assessment. Also, knowing the level of sensitivity and how it will be processed. What are the processing activities that will occur when it's in the US?

Third, it's important to identify the transfer tool that you'll be relying on. Beverley, you've talked a lot about the templates and how they're modal, and this is going to be for determining the next step, identifying what the relationship is between the parties. Is it a controller-to-controller, controller-to-processor, processor-to-processor, or a processor-to-controller?

Next, of course, is conducting that transfer impact assessment that we just talked about. And again, we mentioned, based on the results of your assessment, determining whether you'll need to add supplementary safeguards to mitigate any potential risk to the data. So, the European Data Protection Board, or the EDPB, published some guidelines that are very helpful for this process. And they include examples of technical safeguards that can be added to the clauses. For example, encryption or pseudonymization.

Last step, maybe, is to continue to reevaluate and monitor any changes to your processing activities, or the type of data you're transferring, or any laws that might have or been enacted since the time you entered into these clauses. And as you had stated earlier, don't forget that transfers from the UK will also need a separate assessment.

Last question, maybe. Beverley, since these transfers often include employee personal data, are there any additional considerations that we should be thinking about?

Beverley (21:46):

Absolutely, Mary. We've already talked about encryption or pseudonymization, particularly where sensitive data is involved. I'd also say that, and not many are

aware of this, the data subjects are actually entitled to see evidence of the adequacy mechanism that the organization is using.

So, for example, if you are relying on the model clauses, the SCCs, it may be preferable to have a separate set of arrangements and agreements for employee data, as opposed to customer data and supplier data. The reason being, you might not want to show your customers or your suppliers your contract model clauses in respect to your employees, and vice versa.

And also, something that I've experienced with the US, particularly where the head office is based in the US and there are subsidiaries in the EU, just be aware that intragroup transfers are also subject to the same regime, even though they are companies within the same group. This often gets missed, and entities assume that because they're in the same group, they're not subject to the regime of the GDPR or the transfer of personal data, and they are.

That's where binding corporate rules can come in handy, but a lot of organizations tend to rely on the model clauses instead, particularly in the ever-evolving world of data protection, where you could spend a year or so implementing the binding corporate rules, only to find that the law has overtaken them at the end.

Mary (23:16):

That's a great point, Beverley, about intragroup transfers. This is definitely an issue worthy of more discussion. But hopefully, we've given you listeners some helpful, basic information.

The use of the new model clauses are going to gain momentum, and as they do, we'll likely see more implementation guidance from the EDPB, especially with respect to conducting the transfer impact assessments. So, this is an area we definitely recommend that clients monitor closely.

Beverley, thanks so much. I always enjoy talking with you.

Beverley (23:45):

Thank you, Mary. It's been a delight to be with you and to talk about the transfers of personal data across the pond. Thank you.

Alitia (23:54):

Thank you for joining us on We get work™. Please tune in to our next program, where we will continue to tell you not only what's legal, but what is effective.

We get work™ is available to stream and subscribe on Apple Podcasts, Google Podcasts, Libsyn, Pandora, SoundCloud, Spotify, Stitcher, and YouTube. For more information on today's topic, our presenters, and other Jackson Lewis resources, visit JacksonLewis.com. As a reminder, this material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client-lawyer relationship between Jackson Lewis and any recipient.

Transcript provided by Rev.com