Podcast

The EU-US Data Privacy Framework: Transferring Personal Data Under the New Privacy Shield

By Mary T. Costigan &

September 27, 2023

Meet the Authors

Mary T. Costigan

Principal

908-795-5135

Mary.Costigan@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity

Details

September 27, 2023

Now that the European Commission has published the new EU-US Data Privacy Framework, it will be easier for organizations to transfer personal data from the EU to the United States.

Additional speakers: Dr. Michael Witteler, Partner at Pusch Wahlig Workplace Law

Jackson Lewis P.C. · The EU-US Data Privacy Framework: Transferring Personal Data Under the New Privacy Shield

Listen on Soundcloud

Listen on Apple Podcasts

Listen on Spotify

YouTube

Transcript

Alitia Faccone:

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

Now that the European Commission has published the new EU-U.S. Data Privacy Framework, it will be easier for organizations to transfer personal data from the EU to the United States. On this episode of We get work™, we discuss the new framework, its similarities to the former EU-U.S. Privacy Shield Framework, its application to transfers of employee personal data, and the certification process. Our hosts today are Mary Costigan of counsel in the Berkeley Heights Office of Jackson Lewis, and Dr. Michael Witteler, head of data and privacy, and partner at Germany's Pusch Wahlig.

Both firms are members of L&E Global, a global alliance of labor and employment firms. Mary maintains a certified information privacy professional designation with the International Association of Privacy and is a core member of the firm's privacy, data, and cybersecurity practice group. She advises organizations across various industries and jurisdictions on a broad array of data privacy and cybersecurity matters, including breach response.

Michael has more than 20 years of experience and advises employers on a wide range of issues relating to the handling of personal employee data, the handling of data breaches, and the permissibility of transmitting data to other group companies outside the EU. Mary and Michael, the question on everyone's mind today is, how can employers navigate the complex and challenging task of data transfers between the EU and the U.S. and, "How does that impact my business?"

Mary Costigan:

Thank you, Alitia. I'm pleased to be speaking with Michael today. A little background on how Michael and I know each other. As Alitia mentioned, both Jackson Lewis and Pusch Wahlig are members of L&E Global. Due to the growing number of global data protection laws and the compliance challenges these laws present to HR data, L&E created a data protection group to help member clients. Michael and I are both part of that group, which meets periodically to discuss emerging issues.

Michael, it's always great to speak with you and hear the EU perspective on data protection. I was hoping that we could start off with a bit of legal background and history on transatlantic data transfers, how we got here, and what was done in the past. Michael, since this is an EU-driven framework, perhaps you can start us off.

Michael Witteler:

Yeah. Thank you very much, Mary, for the introduction and for inviting me to speak here today on the Jackson Lewis podcast. It's a pleasure for me. You are right to ask what is the legal background and why we need the Data Protection Framework here in Europe, or to be precise, in the member states of the European Union, which are 27 European countries. To find out, we need to take a look at the GDPR.

The GDPR is the central law for data protection in Europe. There are other regulations at the level of the 27 EU member states, but the framework is the GDPR, and it is binding for all member states. It contains regulations for the transfer of personal data from a member state, for example, Germany, France, or Portugal, to a third country, for example, the United States of America.

Why do we call it a third country and not a second country? Well, of course, because the transfer between controllers or processors within the EU, European member states, whether was in one country or from one EU country to another, is not subject to any additional requirements. This is different with regard to the third countries, which are all non-EU member states, so it means also the United States.

Well, the central objective of the regulations can be found in Article 44, sentence two, which I would like to quote. It says, "All provisions in this chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this regulation, the GDPR, is not undermined." The GDPR, or to put it more precisely, the European legislator, would like to transfer the European level of data protection when transferring data to a country whose level of data protection is lower as we

understand it. We are exporting European law, as you are doing in the U.S. in other areas, so we are learning from you.

We ask, in Europe, two questions. First, does the level of data protection in the third country correspond to that in the EU, or if it does not, how can we ensure a sufficient level of data protection? For this, the GDPR holds some possibility, which we will discuss later. What do our listeners know from the past? Well, we had Safe Harbor for a long time. Then the European Court of Justice came along and ruled that Safe Harbor violated European law, so it was history.

After a short period of uncertainty about how to transfer data from Europe to the U.S. or other third countries in a legally secure way, the Privacy Shield followed. This was an agreement between the European Union and the U.S., and it was agreed during the time of President Obama. Once again, the European Court of Justice ruled that this was not sufficient. The main reasons were that in the European view, authorities in the United States can access data of EU citizens too easily, and secondly, that EU citizens do not have effective legal protection in the U.S.

It is important to know that there's a fundamental right in Europe to an effective remedy and a fair trial. That's the background for the second opinion of the European Court of Justice. Well, these decisions by European Court of Justice have prompted the United States and the EU to negotiate and enter into agreements to address these concerns, the so-called Data Protection Framework. Well, back to you Mary. How does the DPF work and what is required to certify to new DPF?

Mary Costigan:

Thanks, Michael. Overall, the key difference between the invalidated Privacy Shield and this new framework, the DPF, relates to the U.S. government's commitment with respect to national agencies accessing the transferred data, and also increased opportunities for aggrieved data subjects to seek judicial redress in the U.S. For U.S. organizations, the certification process itself hasn't really changed. It's very similar to the Privacy Shield certification process.

The DPF is also administered by the U.S. Department of Commerce, as was the Privacy Shield, and to participate or certify to the program, U.S. organizations must take several steps that include first submitting a certification application through the U.S. Department of Commerce portal. That certification application is going to include information such as demographic and contact information, information about the nature of the personal data transfers, the organization's processing purposes as it relates to that transferred data, how the organization will verify compliance. Will it be self verification or third-party verification? And other similar information.

The organization must also select an independent resolution mechanism to handle any data subject complaints about the processing of data, the processing of transferred data, and it must also publish a privacy policy. This privacy policy embraces the DPF principles, which are fair information processing principles, and it must publicly commit to adhering to these principles.

Then finally, to stay in the program once certified, the U.S. organization must renew its certification

annually. For those organizations that happened to retain their certification under the Privacy Shield after it was invalidated, they can transfer this certification to the DPF, but it must be transferred before October 10th. The process for that includes basically updating their certification, their privacy policy, and any public representations to reference the DPF, rather than the Privacy Shield.

Michael Witteler:

Does HR data receive special treatment?

Mary Costigan:

Yes. The DPF also applies to HR data. In fact, there are additional obligations for U.S. organizations that specifically receive HR data transferred in the context of the employment relationship. A few examples of these additional obligations. While the U.S. organization may select an independent dispute resolution mechanism in the U.S. to resolve any data subject complaints about their processing, for purposes of this HR data, it must resolve any HR-related complaints through the appropriate EU supervisory authority.

Also, when certifying, the U.S. organization must annually commit to cooperating with the local member state supervisory authority, rather than the U.S. independent dispute resolution mechanism. In addition to committing to cooperating, they must agree to cooperate fully with an investigation and also agree to comply with any resulting advice or remedial actions suggested by the supervisory authority.

Another difference is that while the U.S. organization is required to publish its DPF privacy policy, if the policy relates solely to HR data transferred in that employment context, it does not need to publicly publish that policy. Instead, it needs to make it readily available to its employees and notify the Department of Commerce in that certification application as to where that location is.

Michael, are the standard contractual clauses which many U.S. organizations have been using for transatlantic transfers still a viable alternative transfer mechanism? If so, are there also other alternatives?

Michael Witteler:

Before I answer your questions, one more important note for our listeners. Before we check whether the transfer to a third country is okay or not, it must be checked whether the processing of the data is permissible at all, whether in Europe or elsewhere. Only when this question can be answered with yes, we can check whether the transfer to a third country is permissible.

What is not permissible in Europe cannot be carried out in a third country either. That's very important to keep in mind because clients often think if we may transfer the data to the third country, everything is okay, but we must never forget that we also have to check whether the processing itself is permissible at all.

Mary Costigan:

That's a great point. Especially with respect to HR data, which may be subject to more stringent processing rules in member state countries.

Michael Witteler:

Yes. Are there any alternatives? Yes, there are alternatives. The GDPR provides for several options. First, the transfer can be made to a third country whenever there is an adequacy decision by the European Commission. This is now the case for the United States, and otherwise, only for less than 15 countries worldwide. In the absence of a decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46, GDPR lists a number of possibilities. The most important instrument is still the Standard Contractual Clauses, or short, SCC. This is a set of contracts adopted by the European Commission. The contracts must be concluded between the data exporter and the importer, and they must also be observed. It is not sufficient to sign the contracts. They must also be observed. SCCs were mainly used after the legal end of the Privacy Shields In the relationship with the United States. They are still permitted.

Another instrument, especially for multinational corporations, are binding corporate rules. These are rules that the individual companies in the group adopt worldwide, and which must meet certain requirements set out in Article 47 of the GDPR. In Europe, biding corporate rules require the approval of the competent supervisory authority, so they are not used very often, but SCCs are still in use, and perhaps, the most used instrument for the necessary guarantee to transfer data to third countries.

Mary Costigan:

What would the risk be to an organization if they transfer data to the U.S. from the EU without any of these safeguards that you've mentioned?

Michael Witteler:

Well, there are mainly economic dangers. The supervisory authorities cannot only prohibit the transfer of data to the United States, they can also impose fines. Before the GDPR came into force in 2018, fines did not play a major role. They were negligible. That has changed. The fine can be up to 20 million euros or 4% of global turnover, and we keep seeing fines in the hundreds of millions. For example, against Meta or, recently, against TikTok.

In addition, the people affected are threatened with claims for damages. Unlike in the U.S., only actual damages have to be compensated, so the claims for damages are not punitive in nature in Europe. The damages can be very small in individual cases, but in a large number of cases, the amounts add up very quickly. There are mainly economic danger, but also the danger that the

supervisory authority prohibits the transfer of data to the U.S. is a danger for the companies which need the data, or the transfer of data between Europe and the United States.

Mary Costigan:

I have another question regarding other countries in Europe that don't belong to the EU, such as Switzerland. Before, we had the Swiss-U.S. Privacy Shield, but that was invalidated shortly after the Schrems decision invalidated the EU-U.S. Privacy Shield. How does the DPF apply to these other countries?

Michael Witteler:

Well, it does not apply directly, so these countries have to negotiate. If they have a comparable data protection law, they have to negotiate their own agreements with the United States. It is important to know that data protection laws in Switzerland and the UK are very similar to those in the EU member states. Of course, the UK was a long-time member of the European Union and when the GDPR came into force, it was still a member state. They decided to have a new data protection law after leaving the European Union, but it is very similar to the one in the European Union.

For Switzerland, similar. They are very close to the European Union due to all the economic relationship between EU member countries and Switzerland, so they have a very similar data protection law in Switzerland. There's also an adequacy test for both countries in Europe because the use assumes that the level of data protection is similar to that in the EU. As far as we can say, see, there are negotiations between the U.S. and Switzerland on a new DPF. I don't think they have been finalized yet, but it is expected this will not take much longer. This is how it was back in the days of Privacy Shield. Mary, perhaps you can add something regarding the UK.

Mary Costigan:

Yes. The EU-U.S. Data Privacy Framework does not apply to data transferred from the UK to the U.S. However, U.S. organizations who are interested in receiving data from the UK can do so by certifying to the UK Extension to the EU-U.S. DPF, also known as the UK Data Bridge. The UK Extension essentially piggybacks on the EU-U.S. DPF. You cannot certify to the UK Extension separately.

Once you've certified to the EU-U.S. DPF and have been placed on the certified list, you can then extend that certification to UK data by selecting the option to add the UK Extension to your DPF certification. Once you've done this, you can begin receiving personal data from the UK after October 12th, 2023. This means you'll also need to update your privacy policy and public statements to note your certification to the UK Extension.

Michael Witteler:

What are the advantages to U.S. organizations from certifying?

Mary Costigan:

Well, it's going to depend a lot on the type of data transferred and the business operations but, in general, there are several advantages for certifying to the new DPF. Perhaps, the most important is it conserves time and resources, so transferring and reliance on the DPF is going to be much less time and resource-intensive because certifying is a one-time deal. After submitting the certification application and having it approved, after selecting your independent dispute resolution mechanism, and after publishing your privacy policy, all that's required is annual renewal. As I said before, that renewal is based on either self-verification of compliance with the program, or third-party verification of your compliance.

In contrast, if we're going with the Standard Contractual Clauses, that requires negotiating and executing a set of Standard Contractual Clauses with each commercial contract that will involve a transfer of data to the U.S. That can be very labor-intensive and slow-moving if you're an organization that enters into a significant number of commercial contracts that involve a transfer of data.

Also, the Standard Contractual Clauses require that you perform a detailed transfer impact assessment. The DPF does not, so that's another advantage to certifying to the EU-U.S. DPF. Third, as I mentioned before, the self-certification process is just relatively straightforward, unlike the SCCs, which are tied directly to a specific commercial contract, in most cases, that's being negotiated.

There are definite benefits to certifying to the DPF. I've heard a lot of clients express concern about the DPF eventually being invalidated, similar to the Privacy Shield. If the challenge is made again, which is anticipated, it will likely take years to work through the European courts to reach a final decision, and so during that time, this may be a good mechanism to take advantage to. Also, another consideration is that, perhaps, if it does work its way through the courts, during that period, the EU and the U.S. may find more common ground on how to resolve any concerns.

Michael Witteler:

Yes. To summarize, one can say that the DPF makes it easier to transfer data between EU member countries and the United States. There is hope that with the current legal situation in the U.S., the European Court of Justice will not rule that the DPF violates EU law, but we never know.

At the moment, we don't see that many use cases of the DPF in Europe. This is, perhaps, due to the fact that companies wanted and needed to continue transferring data after the end of the Privacy Shield. They have, therefore, often used the SCCs, which continue to apply. Many companies, therefore, do not yet see the need to change this. Since the European Court of Justice will, sooner or later, also rule on SCC, this can change very quickly.

In addition, there are still very many companies that do not even care about questions of legality of transfers to third countries. However, one is of the risk is increasing, so the number of use cases under the DPF will certainly rise sharply. Yeah, we are prepared to all the questions coming from our

clients regarding what has to be done, what has to be observed, and what are the risks.

Mary Costigan:

Michael, as always, it's been a pleasure speaking with you.

Michael Witteler:

Thank you very much.

Alitia Faccone:

Thank you for joining us on We get work™. Please tune into 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.