MAYER | BROWN

Strategic Considerations for Data Privacy Compliance in Tech Transactions

October 27, 2022

Announcer
Welcome to Mayer Brown's Tech Talks Podcast. Each podcast is designed to provide insights on legal issues relating to Technology & IP Transactions and keep you up to date on the latest trends in growth & innovation, digital transformation, IP & data monetization and operational improvement by drawing on the perspectives of practitioners who have executed technology and IP transactions around the world. You can subscribe to the show on all major podcasting platforms. We hope you enjoy the program.

Julian Dibbell
Hello and welcome to Tech Talks. Our topic today is "Strategic Considerations for Data Privacy Compliance in Tech Transactions." I'm your host, Julian Dibbell. I am a senior associate in Mayor Brown's Technology & IP Transactions practice. I'm joined today by my colleagues Arsen Kourinian, Josh Cohen and Megan Von Borstel. Arsen is a partner in Mayer Brown's Los Angeles office and a member of the Cybersecurity & Data Privacy practice. Josh is an associate in the Cybersecurity & Data Privacy practice, the Technology & IP Transactions and the Corporate & Securities practices in our Chicago office. Megan is a mid-level associate also in the Chicago office and a member of the firm's Litigation and Cybersecurity & Data Privacy practices.

I think the average person to the extent that they know anything about data privacy laws or think about them, they think about them in the context of direct breaches of those laws, you know, where some kind of personal privacy violation has actually or allegedly occurred, you know, a data breach at a credit reporting agency, say, or improper data sharing via social media company. The average technology lawyer is probably more sophisticated than that and knows that even before you get to that point, companies can run afoul of data privacy laws just in how they enter into a particular transaction with another business, right? But I don't think we're always clear on when and how those laws are implicated in that context. So let me just ask you straight up, how do we know whether data privacy laws are triggered in a tech transaction?

Arsen Kourinian
Thanks, Julian, and hello everyone.

I think the initial question is how are these laws triggered and they're triggered whenever personal information is either received or disclosed by one of the parties that is subject to the deal. Now when you think of personal information, it's important to understand what it exactly means. It's a very broad term. So some common ways you would think of personal information would be things that maybe directly identify someone, such as an email address or a name or a phone number. But the reality is the way these data privacy laws define personal information, it goes well beyond that. So it could include things that might indirectly be linked to information that identifies you, such as someone's IP address, device ID, or, for example, if it's an ad tech deal where there's going to be cookies placed on a website they can monitor somebody's usage of a website.

Now in those instances, you may never know who that person is. You might never know who the person is affiliated with an IP address or a device ID, but those data sets in and of themselves are actually personal information, and so whenever personal information either is being received by you as a party to the agreement or you're going to be disclosing or making available personal information to another party to the deal, it is important to understand what data privacies are triggered and what the implications are and what terms you would need in the contract for that.

Julian Dibbell
Okay, so laws are triggered, but what laws, right? I have heard there are over 150 data privacy laws around the world. How do we determine which country's data privacy laws are triggered for compliance purposes?

Megan Von Borstel
Well, Julian, there is no one-size-fits-all solution to this, unfortunately; but we do have some guideposts to help us out. So, for starters, a couple to understand: whose personal information is involved here? For example, if there's EU residents' or US residents' data that is being processed. It's also helpful to know where the data is actually being stored. So if it's in a cloud in Brazil or if it's located in Canadian servers, for example, those kind of questions simply give us an idea of which of these data privacy laws are going to be triggered? And then that requires us to address certain countries' specific requirements. I'm talking like cross-border data transfers, processor service provider terms, and then we take it from there.

Julian Dibbell
Okay, and then besides countries we have within the US, we have state privacy laws to worry about, right? I've heard there are some US state privacy laws that are kicking in next year. Which

of those should businesses have on their radar?

Megan Von Borstel
You heard right. There's five US states that have passed pretty comprehensive privacy laws that are going to become effective at various points next year. So the states to look out for: Virginia, Colorado, Utah, Connecticut and then also California. Now that might seem like a lot. But, fortunately, many of these laws have overlapping requirements and consistent regulatory schemes, typically modeled after Europe's general data protection regulation, also known as the GDPR. But there is one law, California's law, the California Privacy Rights Act, the CPRA, that's quite different from the rest.

Julian Dibbell
How so? What makes it different?

Megan Von Borstel
For one, the CPRA does not closely track the GDPR. So under CPRA in California, we're looking at an opt-out model. The consumers have the right to opt-out of their processing as opposed to an opt-in consent model under the GDPR and those other state laws. So it's going to create a few unique regulatory obligations for businesses.

The other reason it's pretty different is it's considerably broader than the other state laws. So the CPRA is currently the only state US privacy law that's going to apply to employee data, HR data and business-to-business data.

Under its predecessor, the CCPA, there was an exemption for both of those types of data, but that's set to expire on January 1st, 2023. So we're seeing a lot of clients, a lot of companies, revamp their approaches to their compliance with this law.

Julian Dibbell
If a business is evaluating whether they are subject to the CPRA, what are the triggers that could apply?

Megan Von Borstel
If you are a for-profit company, you do business in California, then it's important to take a close look at the threshold requirement.

At a high level, the CPRA regulates four different types of entities. We've got businesses, service providers, contractors and third parties. Business is the relevant one under the CPRA if you're a data controller. You're the one who's determining why the data is collected and how it's going to be used. The company can qualify as a business if they are for-profit entities that does business in California and then they meet one of three critical thresholds. So that's going to be (1) do they have gross revenues in excess of 25 million a year; (2) do they buy, sell, share the personal information of at least 100,000 California consumers or households; or (3) they derive

50% or more of their annual revenue from selling, from sharing that California consumer personal information. If you meet any one of those three triggers then you would qualify as a business and be subject to specific requirements under the CCPA and the CPRA.

Julian Dibbell
That is just the businesses, the first category of entities, what about the others that you mentioned?

Megan Von Borstel
Right. So you've also got this other bucket, service providers. Those with the companies that are processing information on behalf of another business. They could also be subject to the CPRA and other state laws. You are going to have to have specific terms in your contract as a vendor in that case. There's also third parties also typically process the information or they share the information downstream. They are going to have fewer restrictions on how they use that data.

Julian Dibbell
Okay, a lot going on there in California. What about outside the United States? What are we seeing?

Megan Von Borstel
Fewer developments, fortunately. In Europe, the prevailing privacy law remains the GDPR post-Brexit. We've got the UK GDPR in the UK. So while the GDPR is not as new as the US data privacy laws, there are still interesting regulatory developments in that space. Most notably, we're seeing a lot of scrutiny around the ad tech space that Arsen mentioned previously. The use of cookies and digital advertising has led to eight- and even nine-figure fines from data protection authorities in the past year or two for failure by big tech companies to fully disclose their advertising cookies and give consumers their informed choice around their data.

Julian Dibbell
So, for these laws, what would trigger a company being subject to them, to the GDPR UK and the EU?

Megan Von Borstel
In that case would be looking at mirror triggers, so the GDPR and the UK GDPR through a company can become subject to those laws in one of two ways really. The first is that they have an established presence in the EU, so a branch or an office, regardless of where the data they're processing is located.

For the second way, if they're a company that's not necessarily in the EU, but they offer goods or services, either paid or free, to individuals located in the EU or otherwise monitoring the behavior and they're going to become subject to both of those laws.

Julian Dibbell
We've sorted through what kind of personal information is involved and then which countries' laws are triggered. So now you're sitting down to do your transaction. What provisions are you going to need to include in the agreement to address these laws, Josh?

Josh Cohen
That's a great question, Julian. So for starters, we need to know the nature of the relationship between the parties. So the first party to know is the data controller, which is basically the entity that owns or makes decisions about the personal information and its possession. And there are transactions where there's a data controller who's transferring personal information to another party, which will essentially have free reign over that data for its own usage and purposes.

The recipient here would be another data controller, or what we call a third party, depending on the terminology under the given data privacy law. And in these scenarios there are often limited terms that need to be included in the agreement. We can call these controller-to-controller terms.

For the contract terms, you would want to include representations that both parties will comply with applicable data privacy laws and their collection, processing, and use of the personal information, and that both parties will cooperate and assist each other with discharging their legal obligations.

There are other provisions to consider as well, like indemnification and some reasonable data security terms and breach notification, to name a few. But typically these terms are more limited in this controller-to-controller data-sharing scenario.

Also, as we'll discuss a little later, if the agreement has a cross-border component, some countries have specific requirements for cross-border data transfers, so those issues would need to be addressed as well.

Julian Dibbell
Alright, first you're talking about controller-to-controller relationships and, and what needs to go into that kind of an agreement. What I see more in my practice is where it's a data processing agreement. When did those come into play?

Josh Cohen
Yes, actually, we frequently negotiate the data processing agreements or DPAs in the context of tech transactions.

So in addition to the scenario in which there's two data controllers sharing personal information, another common scenario is where the data controller transfers personal information to a vendor supplier or a service provider in order to receive some service such as cloud storage or software as a service, payment, processing, you name it. In that situation, the recipient of the personal data is called a data processor, or a service provider, depending on the lingo and the data and the applicable data privacy law.

Before a processor performs any operations on that personal data on behalf of the controller, various laws require those parties to enter into a contract that establishes the details of the processing along with certain required obligations. This contract we call the data processing agreement or an addendum, depending on how it's used. And this DPA sets out how personal data is going to be stored, protected, accessed and used by the processor.

Article 28 of the EU GDPR sets out several required components for DPAs that you're likely to see. These include the processor will follow the controllers instructions when processing personal data. All persons handling personal data are subject to a duty of confidentiality. There's a reasonable data security requirement. The processor must cooperate with the controller to comply with privacy laws and obligations. The processor may be subject to audits. The processor needs to flow down the same level of protection in the DPA with any agreement it has with sub-processors.

At the end of the of the services at the conclusion, the processor needs to return or delete the personal information of the controller. Generally, these GDPR-tailored DPAs are sufficient for most of the US requirements, but there are some additional terms that you need to impose on the recipient entity if you want that entity to qualify as a service provider, a defined term under the California privacy laws. Generally the recipient then cannot sell or share the personal information, and the recipient cannot use the personal information for really any purposes other than discharging their obligations under the services.

Julian Dibbell
That's a helpful set of provisions to keep in mind. You mentioned that we were going to talk about what happens when there are cross-border considerations where data is crossing borders between one party and the other. What about those?

Josh Cohen
Of course, that's another great point. Cross-border data transfers. That's probably one of the most dynamic legal issues in the data privacy field today.

As we previewed earlier in an international transaction, you may have to also consider, in addition to your DPA, you may have to also consider cross-border data transfer issues and the appropriate legal mechanisms for handling these.

So cross-border data transfers are a topic deserving of an entire podcast on their own, but essentially the EU and the UK have said that a data transfer outside of their territory is only automatically legally permissible to recipient countries that provide for an adequate level of data protection.

The EU and UK have provided each other in a few other countries with such an adequacy decision, and notably the US has not received an adequacy decision. There may be one in the works, but that's another topic. For countries that are not deemed adequate, like the United States, and you're transferring data from the EU or the UK to an inadequate country, you'll need to rely on a legal transfer mechanism.

The most common of this, of these is the standard contractual clauses commonly referred to as the SCCs, that are pre-drafted model clauses that you just simply attach to the end of your data processing agreement.

Julian Dibbell
Very helpful, Josh, thank you. Thank you, Megan. Thanks, Arsen, for your insights today.

Listeners, if you have any questions about today's episode or an idea for an episode that you would like to hear about, anything related to technology and IP transactions and the law, please email us at techtransactions@mayerbrown.com. Thanks for listening.

Announcer
We hope you enjoyed this program. You can subscribe on all major podcasting platforms. To learn about other Mayer Brown audio programming, visit mayerbrown.com/podcasts. Thanks for listening.