Law360

Real-World Questions For Better Data Privacy Compliance

*By **Elizabeth Bower, Daniel Alvarez, Philip DiSanto** and **Jill Guidera Brown***

Elizabeth Bower

Daniel Alvarez

Philip DiSanto

Elizabeth Bower

Companies that process personal data have devoted particular attention to their privacy and data security programs in recent years, in part due to several high-profile data breaches and developments in the privacy and data security regulatory landscape, such as the European Union's General Data Protection Regulation. And just as we mark one year since the GDPR went into effect, many of those same companies have turned their attention to complying with the California Consumer Privacy Act, which goes into effect Jan. 1, 2020.

Companies should now thoughtfully consider and reconcile the requirements of the GDPR, CCPA and other data protection laws when developing their privacy and cybersecurity programs. But developing policies and procedures to comply with privacy and data security laws is just the first step. Companies should ensure that their actual business practices align with those policies and procedures as drafted. In addition, companies' stakeholders — from the frontlines to the C-suite — should be equipped to handle thorny questions that arise when dealing with personal data, such as:

1. How can you get your business' data from point A to point B, particularly when moving cross-border?

2. Can you use customer data for purposes that differ from the purpose for which it was collected?

3. What changes to the mergers and acquisitions due diligence process are needed in light of international data protection laws?

To help companies think through their approaches to these tough questions, we've developed three common scenarios that test how the rubber meets the road in privacy and data security planning.

1. What is the best approach to ensure that any cross-border data transfers out of the EU satisfy the rigorous requirements of GDPR?

A U.S.-based IT infrastructure company provides its services to companies in the EU, which use the service to process personal data subject to GDPR. How can the U.S.

company transfer its EU clients' data out of the EU to its servers in the U.S. in a way that satisfies the rigorous requirements of GDPR?

What are your options?

The GDPR requires there be a mechanism in place to safeguard data when transferring cross-border. Two widely used options are the European Commission's standard contractual clauses, which can be appended to any contract and govern the handling of any personal data, and the EU-U.S. Privacy Shield Framework, a self-certifying data protection framework managed by the U.S. Department of Commerce. Businesses that regularly transfer data overseas, such as those with operations both in the U.S. and abroad, can consider putting binding corporate rules into place to govern such intercompany transfers.

Does European data need to leave the Europe?

One option is to simply leave the data in Europe. Data that is not transferred outside of the European Economic Area, even if it is transferred between different European countries, does not need the additional protection of either Privacy Shield or the model clauses. And EU-based customers may prefer that their data stay in the EU. As such, companies should evaluate their options for — and weigh the risks and benefits of — keeping the data in the EU.

What is the scope of your cross-border data transfers?

If your company has a limited number of customers transferring data from the EU to your U.S. servers, and you do not envision significant EU expansion, signing model clauses with the relevant customers may be easier to manage than undertaking the Privacy Shield self- certification process. In contrast, organizations with significant cross-border traffic may find that the one-time effort for Privacy Shield certification may be a more efficient way to achieve compliance than managing numerous contracts and ensuring there are model clauses appended to all those contracts as appropriate.

Where are you transferring data to?

The Privacy Shield program is limited in scope to cross-border data transfers between the EU and the United States, but model clauses can be used for data transfers out of the EU to any country that does not already have an independent adequacy finding. If the bulk of your cross-border data traffic is between the EU and U.S., Privacy Shield may still be an appropriate solution. However, if a significant percentage of your traffic flows involve transfers to countries other than the U.S., you may need model clauses, anyway.

Understand the Details

While Privacy Shield and the model clauses generally are designed to accomplish the same thing — protecting the rights of EU data subjects when their data is transferred out of the EU — the details of each approach may be different. For example, both the model clauses and Privacy Shield provide individuals with an opportunity to seek redress for alleged mishandling of their data.

Under the Model Clauses, such complaints may be referred to a mediator, or may be brought in the courts of the European member state in which the data exporter is established, but under Privacy Shield disputes are typically settled via arbitration, often in the United States. Likewise, Privacy Shield and the model clauses both anticipate onward transfer of the data to additional parties, but the Privacy Shield requirements are more clear and concise in how to accomplish that.

2. Can you use the data collected about customers in new ways?

A retail company has launched an application that will supplement existing services and provide new ways to engage with its customers. The application is designed to provide weekly updates of new products, as well as push notifications to preidentified customers when there is a product launch that the customer finds interesting. After successful launch, the company finds that the data collected by the application can be processed to derive significantly more information about customers than anticipated. Now the company wants to use that data to do more for its customers, including offering more personalized products and services.

Will the new processing actually involve personal information?

Most privacy laws apply only to, or only restrict the use of, personal information (sometimes termed personally identifiable information or personal data). However, personal information has a broad range of definitions under applicable laws and regulations. In some cases, anonymized or aggregated information may fall outside the ambit of data protection laws. Accordingly, it is critical to identify the types of information needed for this new processing — and particularly whether the data is de-identified or aggregated — to assess any potential restrictions on its use.

What does your privacy policy say?

Any new forms of processing should be checked against your current privacy policies and the representations your company has made to customers and app users. If your newly contemplated processing activities fall outside the uses your company previously disclosed to customers, you may be obligated to inform them of these changes, and may be limited to using only data collected after you updated your privacy policy for the newly disclosed uses. According to Federal Trade Commission guidance, companies are expected to provide consumers the ability to affirmatively opt in before using information that has already been collected in a manner different than initially disclosed.

Are there any limits imposed by applicable privacy laws?

Using consumers' personal information is typically governed by applicable privacy laws, some of which are more restrictive than others. For example, the GDPR requires companies to justify their processing of personal information under one of six lawful bases, and document and disclose the analysis underlying that justification, before engaging in a particular processing activity. And under California's Consumer Privacy Act, a wide swath of activities will be considered a "sale" and subject to an opt-out requirement. Companies will need to take appropriate steps depending on the applicable law's requirements.

What exactly does this new processing entail?

Privacy laws and regulations not only apply to particular types of information, but to various uses of that information as well. For instance, processing customer information for email marketing purposes could fall under the purview of the Controlling the Assault of Non- Solicited Pornography And Marketing, or CAN-SPAM, Act. And the FTC has issued guidance on online advertising practices. The company would need to ensure that any proposed activities do not fall within the purview of these kinds of laws and guidance, or at least ensure that the activities conform with any applicable requirements.

3. How can companies share diligence materials that include personal data of EU residents while complying with GDPR?

A U.S.-based software company is considering the sale of a portion of its business that may include personal data of EU residents (either its employees or customers or both). Bidders will need to perform diligence on the company's records and systems to make valuations and submit bids, but the diligence may involve the disclosure of personal data protected by GDPR.

When do the bidders need each respective piece of information?

While some documents or data might need to be provided up front, it may be appropriate to hold others back until later stages in the bidding process. This would reduce the need to require every potential bidder to sign a GDPR-compliant data transfer agreement.

Does the information need to be disclosed in its current form?

One way to avoid running afoul of the GDPR is to avoid disclosing personal data. Where possible, consider redacting personal data or providing documents that do not contain personal data.

Do the bidders need access to personal data?

The GDPR typically requires data sharing to be accompanied by a data processing agreement, or DPA. The company can consider executing a DPA with each bidder with which it shares personal data. These agreements memorialize the bidders' obligations, such as having in place appropriate safeguards to protect personal data, and notifying of security incidents involving that data.

Can the data be reviewed without leaving the EU?

If bidders (or their counsel) have EU-based offices or personnel, having them review the data in the EU might be preferable to transferring it outside the EU. Keeping the data in the EU avoids the need for a GDPR-compliant cross-border transfer mechanism.

Has notice been provided to data subjects about the possibility that their data might be used in this way?

The GDPR's transparency obligations require the company to provide notice to data subjects regarding how it will use and disclose their data. Companies can consider including in their privacy policies and employee handbooks notice that personal data could be disclosed as a part of a transaction.

In light of the constantly evolving technological and regulatory landscape, privacy and data security compliance will continue to be an area of significant focus for compliance departments and general counsels' offices in years ahead.

Elizabeth Bower and Daniel Alvarez are partners at Willkie Farr & Gallagher LLP. Philip DiSanto and Jill Guidera Brown are associates with the firm.

The authors and their Willkie colleagues regularly contribute additional real-world privacy and data security compliance scenarios to Willkie's Compliance Concourse app.

This article was first published in Law360 on June 11, 2019.