The Privacy Advisor

Original reporting and feature articles on the latest privacy developments

Updating your vendor agreements to comply with GDPR

Lei Shen, CIPP/US

Rebecca Eisner
The Privacy Advisor | Mar 28, 2017

If you have been keeping up with the upcoming EU General Data Protection Regulation, you are likely already aware of the myriad steps that you must complete within your organization before May 2018 in order to comply. For example, you may need to appoint a data protection officer, depending on the types of processing your company conducts. But another important and potentially time-consuming step that you need to complete is the review of your agreements with third-party vendors that will have access to your EU personal data to ensure those agreements comply with the GDPR. Even if your agreements already comply with the EU Data Protection Directive, you may still need to update those agreements to meet the new requirements of the GDPR. This article discusses some of the issues to consider as you review your vendor agreements for GDPR compliance. *Editor's note: Alexandra Ross recently wrote on a similar topic in the March edition of The Privacy Advisor.*

Article 28

Article 28 of the GDPR includes a list of items that a controller must include in its contracts with its processors that will have access to EU personal data. Some of these requirements are already requirements under the Directive (e.g., the requirement that the processor only process personal data on documented instructions from the controller, and the requirement to have appropriate security measures in place), so your contracts should already cover them if you are already complying with the Directive.

However, Article 28 also adds new requirements that you will need to include in your third-party vendor agreements. For example, you may need to add requirements for the vendor to assist you in complying with your various obligations in Articles 32 to 36 of the GDPR. These obligations include assisting you with notifying a supervisory authority or a data subject of a data breach and assisting you with carrying out a data protection impact assessment.

You should also make sure that your vendors are required to either delete or return all the personal data to you, at your option, after the end of the services relating to such processing, and delete any existing copies of the personal data unless otherwise required by EU law. In addition, your vendor must also make available to you all information necessary to demonstrate its compliance with its obligations under Article 28 of the GDPR, and allow for and contribute to audits by you or another auditor mandated by you.

Definitions

If the definitions in your current agreements were based on the Directive's definitions, you may need to update those definitions to reflect the revisions being implemented by the GDPR. For example, the GDPR revises the definition of "personal data" to include online identifiers and location data as well as a reference to genetic factors and updates the definition of "sensitive personal data" (or "special category personal data") to include genetic data, biometric data, and data concerning sexual orientation. The GDPR also changes or adds other definitions, including the definition of "consent" and the term "genetic data."

Data breach

The GDPR adds a data breach notification requirement, and if your agreements already comply with U.S. law, they likely already contain such a requirement. However, it's important to note that the scope of U.S. data breach notification laws and the GDPR are very different. In the U.S., generally only limited sensitive personal data, such as Social Security numbers, financial account numbers, and other information that may subject a user to identify theft, are covered by the state data breach notification laws. Under the GDPR, however, all personal data will be covered by the data breach notification requirement. This includes a breach of any business contact information that is subject to the GDPR. Therefore, you may need to expand the scope of your vendor's breach notification obligation.

In addition, several U.S. data breach notification laws define a security breach to include a risk of harm consideration. For example, Arizona's data breach notification law defines "security breach" to mean "an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information … that causes or is reasonably likely to cause substantial economic loss to an individual." While the GDPR has a risk-of-harm consideration with respect to the controller's obligation to notify the supervisory authority and individuals, it does not have this risk-of-harm consideration for processors. Rather, a processor must notify the controller without undue delay after becoming aware of any personal data breach.

Liability and risk coverage

Given that the GDPR significantly increases the possible fines to the greater of €20 million or 4 percent of a company's annual worldwide turnover, vendors will likely push back on the current limits of liability, indemnities, and other similar clauses to address the new risks. It will be some time before we may determine a reasonable and market standard approach to the appropriate allocation of risk and financial responsibility for such fines as between customers and third-party processors. It will be necessary for data controllers and data processors to

examine their insurance policies, coverages and exceptions to determine the extent to which liability and fines for data breaches and other GDPR obligations may be the subject of insurance coverage.

Privacy Shield

If you are receiving personal data from the EU as a Privacy Shield-certified entity, you will need to evaluate your agreements to ensure they comply with the Privacy Shield's onward-transfer requirements. For example, the Privacy Shield requires that third-party agents that will be receiving EU personal data from you provide the same level of privacy protection as is required by the Privacy Shield principles, among other requirements. If you did not certify to the Privacy Shield before Sept. 30, 2016, then you will need to ensure that your vendor agreements comply with these onward transfer requirements before you may certify.

Directive

The changes above assume that your contracts are already compliant with the requirements under the current Directive. If you are currently not subject to the Directive but will become subject to the GDPR due to the change in territorial scope (e.g., you are established outside of the EU and have no operations in the EU, but will be offering goods or services in the EU or monitoring the behavior of data subjects in the EU), you will need to make additional changes to your vendor agreements to ensure they comply with the GDPR. For example, you may need to add security requirements, subcontracting restrictions, and other similar requirements that are already covered by the current Directive.