DOES YOUR COMPANY (INCLUDING SUBSIDIARIES OR AFFILIATES) HAVE EMPLOYEES IN THE EU?

Employee data exposes you directly to the GDPR, but so do any contractors, vendors, and other third parties.

If you can’t identify your third parties that process your data, it’s time to immediately inventory vendors. Third-party risk is very high under the GDPR. Your company is responsible for any EU data they process, third parties, whether you know it or not.

DOES YOUR COMPANY OFFER GOODS OR SERVICES (INCLUDING FREE ONES) TO CONSUMERS IN THE EU?

Offering goods or services to individuals who are in the EU directly exposes you to the GDPR. As soon as you email a newsletter, or ship products to EU consumers, the GDPR applies to your company.

If your company does not target EU consumers, the GDPR may not apply to you. But remember that it might apply because of other EU data—for example, contractors or suppliers.

CAN YOU READILY IDENTIFY ALL VENDORS YOUR COMPANY USES THAT DATA MAY BE TRANSFERRED TO?

If your company processes EU data, you are responsible for managing any vendors you rely on that process data. Any related stipulations must be contained in written, contractual language.

DO YOU KNOW HOW THE GDPR DEFINES PERSONAL DATA?

Personal data is defined extremely broadly as anything that could be used to identify a person. A recording of someone’s voice, for example without a name or other traditional personally identifiable information (PII)—qualifies as personal data under the GDPR.

CAN YOU READILY IDENTIFY THE LOCATION AND PROCESSING ACTIVITIES OF ALL EU PERSONAL DATA IN YOUR COMPANY?

If EU authorities knock on your door, one of the first things they’ll ask for is a record of processing activities detailing these locations. Make sure this record is comprehensive and maintained on an ongoing basis.

DO YOU HAVE AN INCIDENT RESPONSE AND BREACH NOTIFICATION PLAN AND TEAM IN PLACE THAT CAN SUPPORT A 72-HOUR NOTIFICATION REQUIREMENT?

Having a plan in place is a great start. Make sure to practice it on a regular basis by running tabletop exercises, for example. Also make sure that your vendors know that they need to notify you quickly of any breaches on their systems.

The GDPR requires 72-hour notification, and defines “personal data breach” very broadly including accidental loss, damage or alteration of data. Not meeting this obligation is a direct path to the higher penalties in the GDPR.

HAVE YOU UPDATED YOUR POLICIES AND PROCEDURES (RETENTION AND PRIVACY, IN PARTICULAR)?

Make sure your organization lives by these policies—and can demonstrate that it does, when or if the regulators come calling. Instituting a regular training program and internal audit would be a good practice.

These policies are one of the most important requirements in the GDPR. Key processes must be updated to align to the requirement, and employees should be trained to make sure they understand and follow the new policies.

DOES YOUR COMPANY HAVE A PROCESS FOR RESPONDING TO REQUESTS FOR ACCESS, CORRECTION OR ERASURE OF EU PERSONAL DATA?

Make sure these processes are established and that relevant teams within your organization are familiar with them and practice them regularly. Remember that European data subjects can initiate a complaint process that can lead to intrusive audits and huge fines.

QUESTIONS TO ASK to prepare for EU GDPR

Consider the following questions to determine whether GDPR applies to you, and if so, whether your data security environment is compliant.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate one another. Each member firm is responsible only for its own acts and omissions, and not those of any other party. RSM US LLP is a member firm of RSM International, a global network of independent accounting and consulting firms. © 2019 RSM US LLP. All Rights Reserved.