ALIGN SOURCING WITH THE GDPR

Seven Steps to Accelerate GDPR Compliance with Suppliers

GDPR, SOURCING, AND SUPPLIER MANAGEMENT: A PRIMER

What is the GDPR?

The General Data Protection Regulation (GDPR) is the European Union's regulatory framework for protecting personal data — and it will change how organizations around the world handle data privacy. The GDPR gives individuals more control over their data and holds businesses accountable for handling it appropriately. What's more, it does not merely apply to EU businesses, but to all organizations that process the personal information of EU data subjects.

What does the GDPR entail?

The GDPR places new restrictions on how companies use personal data gathered about EU data subjects, making it mandatory for organizations of all sizes to change how they handle data, who they share it with, how they retain it — and it all goes into effect on May 25, 2018. The stakes are high for noncompliance; organizations that do not adhere to the GDPR can be fined up to 4 percent of their annual global turnover or €20 million, whichever is greater.

How does the GDPR impact sourcing?

In a sentence: Third-party vendors and processors pose the biggest risk to companies adapting to the new GDPR regulations. Not only does the GDPR hold companies directly accountable for data privacy practices, but it extends that responsibility to any third-party vendors who touch personal data. Essentially, companies (data controllers) are required to enforce (through contracts), monitor (through process), and document (through audit and controls) how third-parties are meeting these requirements. Sourcing teams will have to address these requirements through contracting, supplier performance management, and ongoing evaluation.

scout™

SOURCING, THE GDPR HERO

The EU General Data Protection Regulation (GDPR) is called "the most important change in data privacy regulation in 20 years." Its implementation heralds a new era of data regulations, and with these changes come myriad opportunities — and obligations — for sourcing.

In most organizations, GDPR compliance will be largely handled by IT and security teams. However, its scope is much broader — and third-party vendor management is the biggest unsolved problem as the enforcement date nears. The GDPR places a strong emphasis on how organizations define and enforce how suppliers can interact with personal data, which, in turn, puts compliance squarely in sourcing's bailiwick. Below are a few ways that sourcing can help drive GDPR compliance and deliver value to the entire enterprise:

Address GDPR requirements pertaining to third-party vendor management.

Become a data detective and track it through the supply chain. Know where data comes from, how it is used, and who it is shared with. Identify vendors who are accessing or processing the personal information of EU data subjects and then go through your supplier base to determine which suppliers and contracts pose the greatest risk to GDPR compliance.

Enforce supplier compliance with the GDPR.

As a data controller, you are obligated to ensure that your data processors (suppliers) are using the personal information of EU data subjects appropriately. It is incumbent on you to both determine which suppliers fall under the umbrella of the GDPR and ensure ongoing compliance through properly phrased contracts and regular reviews.

Partner with IT and your DPO.

Those directly responsible for the GDPR have a mammoth task ahead of them — and sourcing can play a key role by taking responsibility for third-party compliance. With a proactive and structured approach to the GDPR, sourcing can drive value that extends far beyond savings and make a significant impact to the business.

Certain articles of the GDPR are particularly applicable to sourcing. You should be well-versed in the GDPR in its entirety, but here are a few sections to bookmark:

Articles 15-22
Outline the various — and very comprehensive — rights of data subjects.

Article 28
States that any organization doing business in the EU is responsible for all third parties that are processing personal data on their behalf, and thus also accountable for GDPR compliance.

Article 30
Holds organizations responsible for keeping comprehensive records of data processing activities.

Article 32
Requires that organizations (and their partners) take proper security measures when handling and storing data.

SEVEN STEPS TO ALIGN SOURCING WITH THE GDPR

Today's business world is driven by data; it has even been called the world's most valuable resource. Sourcing can take advantage of the GDPR to drive enterprise-wide value that extends far beyond savings. Start with these seven steps:

1. **Reach out to your security and privacy teams** (if you haven't already) to assess the scope of risk related to the GDPR.
2. **Understand your data** — where it comes from, how you use it, and who it is shared with.
3. **Identify and segment suppliers** based on their access to data.
4. **Build questionnaires and workflows** to validate suppliers' compliance.
5. **Review and update contracts** to ensure GDPR compliance.
6. **Update Supplier Performance Management** to include scores for updated contracts and compliance adherence
7. **Build reporting** to assess vendor compliance across the business and conduct regular performance reviews to continue to mitigate potential risks.

SCOUT, SOURCING'S GDPR SUPERPOWER

GDPR compliance is not just an obligation, it is an opportunity for sourcing to shine. By approaching it through the lens of risk mitigation, procurement can both raise its profile and deliver unprecedented value to the enterprise.

To achieve this, sourcing must be empowered to uphold their compliance responsibilities. This means actively segmenting suppliers, proactively managing contracts, and continually providing visibility into which third parties are handling personal data, and how.

Scout's eSourcing platform provides a simple, smart, and streamlined way to ensure GDPR compliance. Look to specific Scout modules to tackle:

Contract Management

Update contracts to ensure that they are GDPR-compliant, and then send these across vendors. Manage contracts from a single, easily accessible repository.

Supplier Management

Perform proper segmentation of vendors based on their access to personal data. Then, validate suppliers by tier and/or segment, and build new workflows to ensure ongoing compliance.

Questionnaires

Collaborate with your organization's security and privacy teams to regularly conduct GDPR-specific vendor survey questions. This will help ensure compliance, and make it easier to report on.

Disclaimer: The content of this white paper is intended to keep interested parties informed of certain developments regarding GDPR for educational purposes only. It is not intended as legal opinion and should not be regarded as a substitute for legal advice.