A Strategic Approach to Vendor-Management Under the GDPR

Alexandra Ross, CIPP/E, CIPP/US, CIPM, FIP

If you're a privacy professional tasked with ensuring your company is in compliance with the upcoming General Data Protection Regulation requirements, one of your main challenges may be communicating the profound shift in how GDPR delineates the roles and responsibilities of "controllers" and "processors." With this shift in responsibility, companies will need to establish more rigorous practices for managing their relationships with vendors who act as processors.

As an example, a global technology company offering cloud services may act as a controller with regard to its employee data and as a processor with regard to its customer data. Under the GDPR, the company would be responsible for the vendors used to manage its EU employee data (in that case, its processors) and the vendors used to manage its EU customer data (in that case, its sub-processors).

It's not uncommon to experience some push-back when it comes to raising the red flag over tighter vendor controls. After all, the burden of vendor management is not an easy road. It can be complex and time consuming. But the business case for compliance with GPPR is clear — the penalties are steep and the collateral public relations damage can have a chilling effect on a company's performance.

So how can you take a pragmatic approach to vendor management under GDPR? Here are some best practices for taming this challenge.

Achieve clarity on legal requirements

Before you mobilize a team to streamline a compliance process, you must have a clear understanding of what the GDPR specifies as obligations to manage processor relationships.

Be sure to examine:

- **Article 28 (1)-(3): Processor Obligations**
- **Article 24(1): Controllers**
- **Article 29: Processing under the authority of the controller or processor, and**
- **Article 46(1): Transfer subject to appropriate safeguards.**

In reading these sections of the GDPR, it becomes obvious companies can't simply outsource the responsibility of data governance and privacy compliance to their vendors. Companies have an obligation to conduct due diligence, have appropriate contract terms in place, and must monitor the services provided by vendors to ensure they are processing data in accordance with applicable data protection regulations. If there is a violation or data breach caused by a vendor, your organization will be liable. (One need only bring to mind the fall-out from Target's high-profile data breach in 2013, in which a relatively small HVAC vendor allowed hackers relatively unfettered access to customer data.)

In a previous IAPP article, Anna Myers, CIPM, CIPP/US, offers a perspective of these issues.

A framework for compliance: people, process, technology & metrics

To amend a quote by environmentalist and entrepreneur, Paul Hawken: "Good [vendor] management is the art of making problems so interesting and their solutions so constructive that everyone wants to get to work and deal with them."

The broad strokes of applying such a constructive and inspiring approach to vendor management include: identifying the right people, formulating a process for interfacing with vendors, leveraging technology to manage the process, and keeping solid metrics for internal and external compliance purposes.

People: A first step is to determine who in your organization should be engaged with vendor selection and management. Someone should be accountable within each business team that utilizes vendors – this may be a chief of staff or VP of a particular functional business or product team. It helps to identify these privacy champions who are responsible for complying with company policy on vendor management and for evangelizing a culture of mindful sharing of data with vendors. While it's great if you have a formal Vendor Management Office, the alternative may be a committee of stakeholders from the procurement/sourcing, legal, privacy, and security departments.

Process: It's important to view vendor management as a lifecycle. It begins with the strategic choice of vendors and should include a formal intake process. Often you'll need to disabuse the notion that many of your business partner may believe – that free vendor services or click through terms are not an issue. Wrong – any processing of personal data by a third-party vendor should be in scope for a GDPR-compliant vendor-management process, regardless of the cost of the service offering. Another common misconception is that these obligations only apply to processors managing customer data. Wrong – processors that manage a company's employee data must also be in scope.

Defining appropriate contractual terms, conducting security reviews, and sponsoring ongoing maintenance and monitoring are part of the cycle. The goal is consistent treatment of data by the company and its processors to maintain compliance with regulatory obligations and promises made to data subjects.

Technology: Ad hoc vendor inventory and contract record keeping is a recipe for disaster. Many companies struggle with compiling and maintaining a complete inventory of vendors and vendor contracts. This is especially true in siloed organizations where there is no central repository of vendor contracts, or where business teams may keep (or not) copies of vendor contracts locally. Ideally, you'll want to have a centralized system which will not only track vendor contracts, but will also provide robust reporting to flag vendors who process personal data, flag vendor-use by geo and alert stakeholders of contract terms with upcoming renewal dates.

Metrics: With the right technology platform in place, your organization will have superior visibility into your vendor management roadmap, and should have no problem tracking progress and measuring milestones. This is key, because you will want to be able to create documentation which demonstrates compliance with GDPR

If you're planning on attending the upcoming IAPP Global Privacy Summit 2017 in Washington, D.C., don't miss the session on "How to GDRP-ify Your Vendor Management Program." This hands-on session will provide guidance on operationalizing the GDPR and improving your vendor management process.

Though the issues and logistics may be complex, it's important to remember that preparation for the vendor management component of GDPR is attainable. A mindful and strategic approach is warranted so that you can properly know your vendors and hold them accountable.