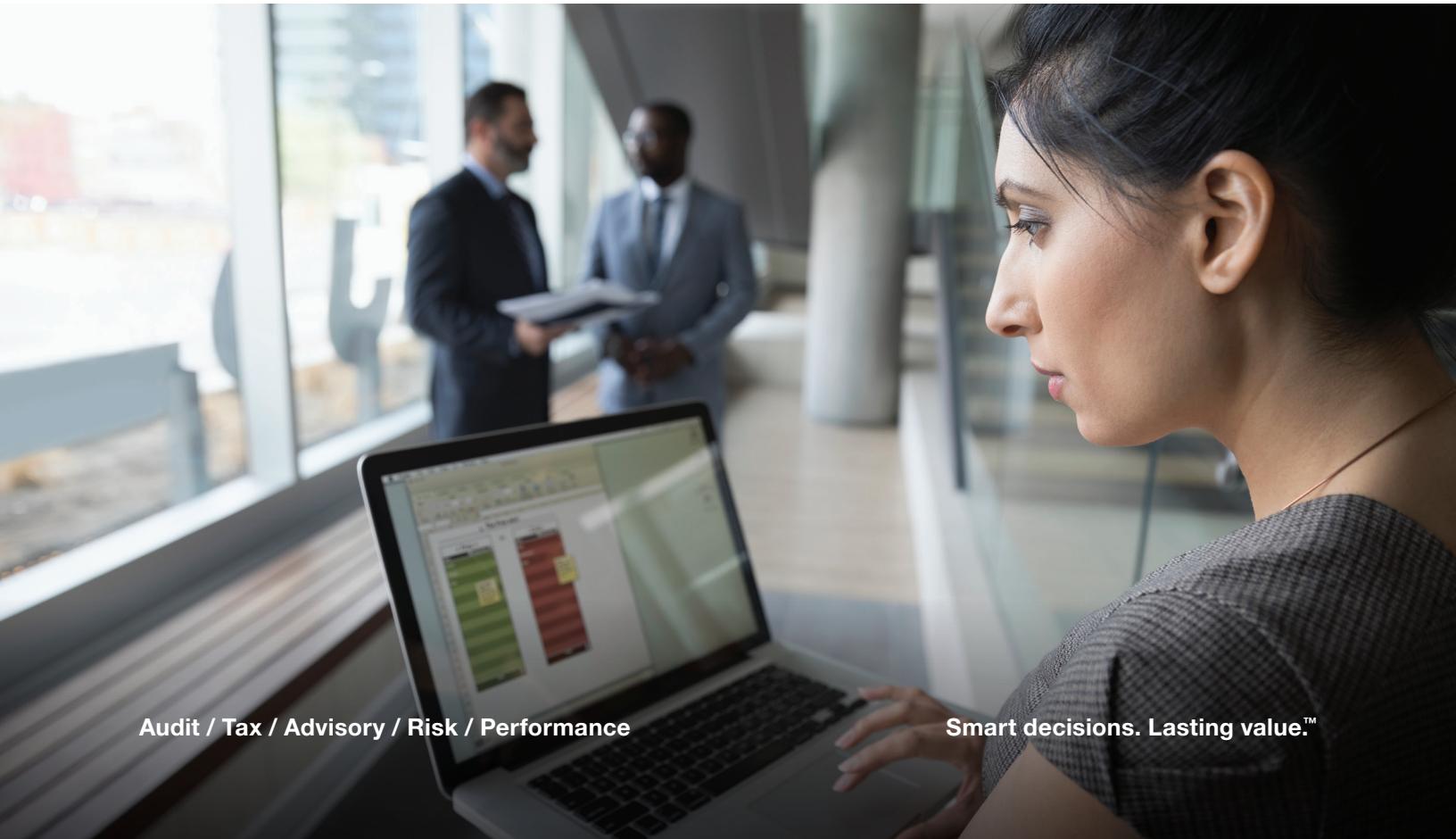




December 2018

Maintaining a Data Inventory

An article by Pamela S. Hrubey, CIPP/US, CCEP



As organizations across the globe work to comply with the General Data Protection Regulation (GDPR), leadership within these organizations understands that compliance can often lead to opportunity under the guise of implementing or revising best practices.

Maintaining a data inventory to meet the obligations within Article 30 related to data-processing records is one such issue. While data mapping and inventories are not specifically called for within the language of the article, building an effective GDPR compliance program based on a comprehensive inventory helps to enable an organization's ability to meet GDPR requirements and to provide a clear vision for ethical data handling that drives value.

Knowledge is power

Organizations rely on data. This reliance encompasses the nature of doing business in the 21st century. For any organization to thrive and get ahead of the competition, data is a key component.

Whether that data is in the form of structured software systems and vast data lakes or unstructured hardcopy documentation, or a blend of both these examples, organizations must have actionable intelligence based on current, accurate data in order to thrive. Throw in regulatory requirements on data subjects'

rights about the storage, processing, usage, and disposal of personal data, and suddenly the vast amount of disparate information becomes potentially unwieldy.

On a high level, the GDPR requires that organizations maintain records detailing information such as, but not limited to, the following:

- Description of the categories of data subjects
- Categories of personal data
- Categories of personal data recipients, including third-party and third-country
- Data retention policies
- Data security policies

For an organization to be compliant with the GDPR, leadership must understand the types of data it possesses. Leadership must also understand how that data is used and shared and have a clear policy-level enforcement on all the critical aspects surrounding that data.

An effective starting point is to build a comprehensive data inventory and data map that identify all of the necessary criteria. While this effort can seem to be an arduous endeavor, putting a high-level data inventory in place should be one of the first efforts when working toward compliance.

Such an approach can initially help the organization deal with data-subject access requests and can lead to an overall improvement in data quality over time as it continues to evolve. The upside is that such an effort can help establish ethical data governance, and it can yield valuable business insights as well.

Quality is key

Effective business operations and compliance programs put in place for regulatory purposes around data privacy and protection depend on the data itself and, more importantly, the quality of that data. High-quality data can provide businesses with in-depth views into market trends, improve overall business strategies, and spur innovation, which can lead to a stronger and more profitable organization.

Building and maintaining a comprehensive data inventory can enhance overall data quality and help create a path to streamline the compliance efforts, which helps in the effort of reducing risk through the creation of an effective controls framework.

Additionally, identifying potential processes that can be automated creates opportunity for better regulatory reporting in both accuracy and efficiency. Improved accuracy supports improved data security. Clear data maps and inventories can support more effective and proactive security measures that address critical issues, such as which specific business processes the data touches and the related risks of that interaction. Complete data lineage capability is also enabled through data accuracy, allowing for a cohesive approach by audit, security, and compliance groups alike.

Compliance through strategy

As organization leadership works to prepare and implement data retention systems and policies that support efforts to protect data subjects' rights, it is important to establish a compliance program that meets GDPR and other regulatory requirements and helps to establish the level of transparency that consumers now demand. Creating a data inventory is the key step to begin this effort, and it can provide a true understanding to companies and consumers about how data is collected, stored, and shared.

A recent survey by the International Association of Privacy Professionals notes that more than 50 percent of companies estimate that they are not yet compliant with the GDPR.¹ The first step to doing so is by gaining a true understanding of the current data environment and then establishing a comprehensive data strategy based on that knowledge. Now, not later, is the time for organizations to take full control of their data and data practices.



Learn more

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

¹ Caroline Spiezio, "Over Half of Companies Are Far From GDPR Compliance, Report Finds," *Corporate Counsel*, Oct. 19, 2018, https://www.law.com/corpcentral/2018/10/19/over-half-of-companies-are-far-from-gdpr-compliance-report-finds/?cmp=share_twitter&slreturn=20180925202756

Reprinted with permission of Information Management. Originally published Dec. 24, 2018, at
<https://www.information-management.com/opinion/a-data-inventory-is-key-to-maintaining-data-privacy-compliance>

crowe.com

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document.

© 2019, 2018 Crowe LLP.

RISK-19003-003D