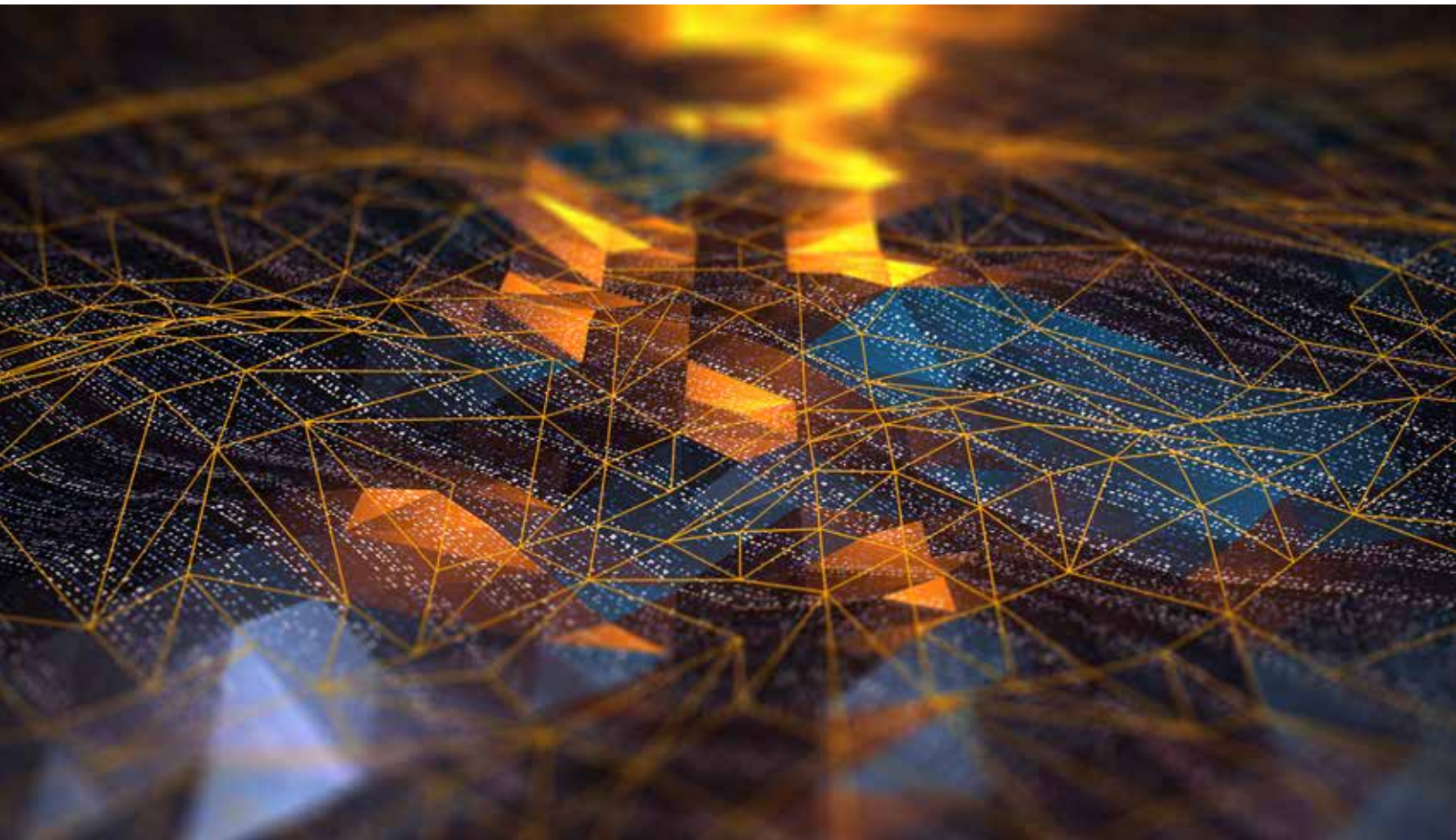


March 2020

Understanding Data Mapping and Responding to Consumer Requests

An article by Mindy R. Herman, PMP, and Peter K. Kalmbach, J.D., CIPP/US



Implementation of the General Data Protection Regulation (GDPR), the *California Consumer Privacy Act* (CCPA), and other similar privacy regulations has left many businesses with the need to rebuild or retool their data privacy and security compliance programs. Increasing data protections and effectively responding to the needs of consumers requires that organizations design, implement, and audit key compliance activities.

Businesses are also challenged by the regulations and requirements of data inventory, data mapping, and responding to consumer requests. In this article, two Crowe professionals explain why data mapping and responding to consumer requests matter and how businesses can best navigate the new regulation landscape.



Privacy regulations are here to stay

When the European Union (EU) implemented the GDPR on May 25, 2018, some U.S.-based organizations without customers or business partners located in the EU were able to avoid complying with the strict and painstaking regulatory requirements. Other organizations with more global business models made progress in their privacy programs.

Specifically related to data mapping, Article 30 of the GDPR requires businesses to track the full life cycle associated with the personal data they hold and to respond timely to requests from consumers regarding the specific data the business holds about the individual. While certain businesses avoided preparing for compliance with the GDPR, avoidance is no longer an option for many businesses with passage of the CCPA, effective Jan. 1, 2020. The CCPA also has requirements to respond to consumers about the use of their data over the prior 12 months.

The jurisdiction of current national, sector, and state regulations allows some companies to delay investing in privacy programs and the associated tracking of their data. Specifically, the CCPA applies to organizations that do business in the state of California and that meet at least one of these three thresholds:

1. Annual gross revenues greater than \$25 million
2. Personal information collected on 50,000 or more California residents annually
3. Revenue totaling 50% or more from selling California resident data

Note that a business does not have to have a location within California for these thresholds to apply. As policies surrounding businesses' use, transfer, and sharing of personal information shift, individuals' privacy rights have moved to the forefront of the privacy debate.

While this article focuses on the GDPR and the CCPA, various countries and sectors already have many regulations in place, and many states have legislation in progress aimed at governing personal data. Specific requirements might vary, but the principles in these regulations are based on common privacy principles.

Building a sustainable privacy program means that companies might need to further address specific topics. Additionally, in building their programs, companies must incorporate privacy principles to honor the legal requirements and the spirit of the regulations established to protect stakeholders' personal information. To be able to handle data from an individual (such as a consumer, data subject, employee, or other covered stakeholder), companies must track what data is collected, used, stored, processed, retained, transferred, archived, and deleted.



Data mapping defined

Data mapping provides a visual representation of the life cycle of personal information as it is used within a defined business process, including notation of the applications, systems, and databases that hold the data and the locations where the data is shared, including third parties.

Establishing a record of the full ecosystem in which personal data is collected, used, stored, processed, retained, transferred, archived, and deleted can be a daunting task for organizations that seek to complete a data map for the first time.

Creating a data map can provide tremendous benefits because the map enables an organization to track data elements from the point of collection through eventual deletion. Data mapping also provides organizations with another lens through which to assess the adequacy of their data security controls.





Responding to consumer requests

Data mapping establishes a line of sight to all the data held by the organization. It also establishes a firm foundation upon which to build processes for supporting requests from consumers relating to their personal data.

Through the GDPR and the CCPA, consumers are granted broad access rights to their data. Consumers have the right to request from a business details about their personal information, including what has been collected, shared, or purchased, and the purpose for which the data is used. Consumers may also request deletion of their personal information.

To prepare to receive requests from a consumer, businesses must have mechanisms by which a consumer can to make such requests. Businesses can use a dedicated email address and a toll-free telephone number or take a more sophisticated approach through use of a tailored self-service portal.

Businesses must also implement well-designed data security programs that include the ability to verify a requestor's identity before providing personal information in response to a specific request from that individual. The information gathered via data mapping permits the business to accurately and effectively respond to the consumer in a timely fashion, defined as within 45 days under the CCPA and within one month under the GDPR.

Why data mapping matters

Data mapping and responding to consumer requests are critical activities for organizations that must comply with the new wave of data privacy and security regulations. Organizations must be able to efficiently build data maps and have a process for addressing consumer requests. To do so, organizations must be able to understand their data processing activities and the rationale for collecting associated information.

Relying on a comprehensive data map helps the organization in the consumer request process. In addition, ideally, the consumer request process should be streamlined, and organizations should be able to draft customizable templates to respond to specific consumer needs.

Organizations also should be able to provide policies and procedures that support the principles of data mapping and consumer rights. Finally, organizations need to pay special attention to confirming the identity of the consumer so that they do not risk a data breach by releasing personal information to an unauthorized individual.

From the consumer's perspective, the situation is clear: Companies must handle consumer data in a manner consistent with the consent the consumer granted for data use. If a company does not have a clear consumer request process or transparent data tracking, it will lose consumer trust.

Getting a plan in place

For many businesses, the new regulations can be daunting. But with a solid plan to address how to best use data mapping and respond to consumer requests, organizations can better support their end users. Technologies can assist, but as one might expect, information integrity and value depend on how companies collect, validate, and map their data.





Learn more

Mindy Herman
Principal
+1 317 706 2614
mindy.herman@crowe.com

Peter Kalmbach
+1 317 208 1985
peter.kalmbach@crowe.com

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.
© 2020 Crowe LLP.