Data Map Now to Ease GDPR Compliance

By David White

The new European Union General Data Protection Regulation (GDPR) formally takes effect in May 2018. The move from the current Data Protection Directive to the GDPR brings with it a whole series of new requirements forcing prudent companies to conduct assessments to identify compliance gaps. Among the key components are the requirements to implement data protection policies, conduct data protection impact assessments and appoint data protection officers.

When viewed along with all of the other changes, it is clear that the GDPR creates a fundamental shift away from simple protection and transparency toward a need to actively manage and control data. This increased accountability for data practices means that most companies will need to make a number of operational changes to meet the new requirements.

For example, businesses will need to significantly enhance their record-keeping activities. Under the current directive, companies who control personally identifiable information are often required to notify their local regulators of their data collection and processing activities. However, each EU member state currently has different notification requirements, which makes compliance particularly difficult for multinational companies or for those that hold data from citizens of multiple member states.

Under GDPR, it will no longer be necessary to submit data processing or transfer notifications or registrations to each relevant regulator, nor will it be a requirement to obtain approval for certain transfers. Instead, there is now an internal record-keeping requirement for all data collection, processing and transfers. The data protection authorities have also reserved their right to audit these activities and the corresponding records. The failure to document has strict penalties for noncompliance. To avoid running afoul, companies will have to start tracking and documenting all of their data gathering and processing activities, both new and existing.

The GDPR's mandatory breach notification requirements are another significant area of change. Data controllers must provide notice within 72 hours of having become aware of any breach that is likely to "result in a risk for the rights and freedoms of individuals." Data processors will also be required to notify controllers "without undue delay" after first becoming aware of a data breach. Given that it can often take weeks or even months to determine exactly what data was accessed in a data breach, these timelines are quite short. Unless companies fully understand their data holdings before a breach incident occurs, they are not likely to meet them.

To address both changes, the most important thing companies can do right now is data mapping. They must spend the time to fully understand exactly what personal information they collect, manage and process, from whom, for what purposes, and where and how it is being used and shared. If they are unable to do this, they cannot even begin to understand their level of compliance and what they need to do to close any gaps. This exercise should also look at international data flows and seek to understand what the legal basis is for legitimizing the transfers. It should also map out all of the service providers who are processing data on the company's behalf and ensure that the proper contractual protections are in place.

Companies need to get moving, however, and not wait until it is too late. Changes to internal business processes and workflows take time to design and implement. If you are not already working on them, you may not meet the looming deadline.

Thankfully, there are a number of technology solutions that can help expedite the process. For example, there are several tools that can crawl across repositories of unstructured data looking for personally identifiable information and other controlled data in order to build data maps and remediation plans. They typically deploy a combination of pattern matching and conceptual search algorithms to home in on the many various types of protected information.

Automated contract review tools can also be a considerable help. They deploy artificial intelligence and machine learning to automate the review of variations in customer and vendor contract clauses, such as confidentiality, data protection obligations, intended uses, legitimate bases for transfer or processing and subcontractor obligations. When combined with traditional data-mapping techniques, these technologies can significantly reduce the time needed for companies to fully understand and document their data flows to meet their compliance obligations. It does not have to be a manual process, and you don't have to do it alone.

David White is a director at AlixPartners LLP, where he advises clients on information governance, information security and electronic discovery. He can be reached at dwhite@alixpartners.com.