

# Is Your Data Discovery Technology Privacy Grade?



# Spirion AnyFind® technology meets the requirements of the most demanding data privacy and security laws.

## New laws set the bar high

The passage of the EU General Data Protection Regulation (GDPR) into law was a watershed event in the world of data protection. The Regulation codified data protection principles, practices, and jurisprudence that had been evolving over the past decade in the EU. In particular, it cited machine-readable data – items like IP and MAC addresses, geolocation information, and RFID tags – as personal data. It also called out so-called “special” or “sensitive” personal data for additional protection, including items such as healthcare data, political/religious views, and trade union membership. The impetus for the Regulation has since spread worldwide, with countries either creating their own version of GDPR (Brazil) or significantly updating existing privacy laws (Japan). The California Consumer Privacy Act of 2018 (CCPA) took the idea of what qualifies as “personal” a step further, adding such items as employment records, Internet browsing history, and records of products/services purchased to the list of personal information. Moreover, the upcoming California Privacy Rights and Enforcement Act of 2020 (CPREA) now defines items such as email messages as sensitive personal data. Taken as a whole, the demands of contemporary data protection laws are significantly higher than those of yesteryear.



## Sifting the wheat from the chaff is surprisingly difficult

The challenge in locating personal data solely with traditional tools such as Regular Expressions (RegEx) or Boolean logic is that they do not understand the context of the underlying search. Instead, they return everything that matches their formula, creating a lost list of false positives to sort through. In fact, a false positive rate of 40% or higher is not uncommon using these tools, creating more work for privacy and security professionals.

In a similar vein, electronic discovery (“e-discovery”) tools have been pressed into service by some to identify personal data in an enterprise setting. However, this too misses the mark. The principal difference between e-discovery and data discovery is that e-discovery is concerned with finding electronic information in a context that advances a legal theory or narrative, such as two companies subtly colluding to defraud the government. Contrast this with data discovery, which is concerned with finding data for its own sake. The upshot of this is that e-discovery technology will miss instances where personal data is located on “orphaned” file servers (and other repositories) that don’t “belong” to anyone involved in litigation. Furthermore, it will miss narrowly defined types of personal data that are not likely to be relevant to litigation, period.



In addition, **Spirion Sensitive Data Engine®** enables you to discover personal data that is unique to your organization, such as user and device IDs as well as identifiers associated with mobile applications and other custom software. Sensitive Data Engine® enables you to discover any personal data that is unique to your organization. With highly customizable context options such as counts, character positions, Boolean requirements, and other conditionals, it is possible to build custom datatypes with near AnyFind accuracy.

## Transform Your Data Discovery into Privacy Grade, Prepare for the Future

The last two years have produced an unprecedented wave of new data protection laws and subsequent enforcement around the world. Since May 2018, the compliance deadline for the GDPR, at least 250 organizations have been punished by regulatory authorities, subjected to fines exceeding €150M as well as the imposition of mandatory injunctions which are costly in their own right. In the U.S., the first CCPA-related lawsuit was filed shortly after the start of the new year in 2020, and multiple lawsuits have followed since. Add to these considerations the routine contractual demands by business partners for precise handling and protection of shared personal data. The result is that companies find they must go the extra mile in identifying and protecting the personal data under their care.

### The Solution?

**Spirion's Privacy Grade Data Discovery included in our Sensitive Data Manager and our Data Privacy Manager. Two, all-in-one solutions available on-premises or in the cloud, to help you build a privacy-first culture.**

**LEARN MORE:**

<https://www.spirion.com/products/platform-overview/>

**Talk to a Spirion data security and compliance expert today: [expert@spirion.com](mailto:expert@spirion.com)**

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at [spirion.com](https://www.spirion.com)