SPIRION™

Buyers Guide: Purchasing Data Privacy and Compliance Software

Offering your customers data security and privacy of their personal sensitive information is no longer a special perk that separates you from your competitors. Because of privacy regulations like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), data privacy and compliance of these regulations should be a top priority for all organizations.

It isn't just new laws that are driving this push toward a privacy-first policy of data management. It's also what consumers are demanding, and this focus on consumer-centric protections is a business driver. According to a **report** from Forrester Consulting, 75 percent of companies recognize that data privacy is a competitive differentiator and 79 percent say adding data privacy and compliance systems is now an IT priority. Adding data privacy solutions, said the Forrester report, businesses are more likely to retain and gain customers, especially as the company adds new IoT and AI devices that collect massive amounts of sensitive and personal information.

But for your organization to protect your customer's data and to be able to meet current and future privacy compliance regulations, you have to know where the data is. Managing data collection, storage, classification, and usage is a daunting task for most companies. Too often data is lost or unclassified, making it impossible for organizations to effectively protect the information or to efficiently meet customer requests to be forgotten, which are the a focal points of many of these data privacy laws.

Data privacy and compliance software allows organizations to more easily find unique sensitive data and classify it. Classifying unique data helps your organization allocate its resources and set priorities, meaning you'll be able to take the most-stringent measures to protect the most-sensitive data.

How do you choose the right data privacy software platform for your company? According to the **International Association of Privacy Professionals** (IAPP), the number of data privacy software companies jumped from 51 in 2017 to over 200 in 2019. Narrowing it down to the right software option seems like a daunting task, but you don't want to sign on with the first name that comes up on a Google search, either. It's like any other software purchase. Before you buy in, you need to have a good understanding of what you need to address. You should have a strong understanding of your industry's compliance laws, as well as state, federal, and international regulations that you may be responsible for following, the data you handle, your storage options, and how to best classify the data coming in.

History of Data Privacy Compliance

In order to make the right decision about data privacy software, it helps to have a better understanding of the privacy laws in place, how we got here, and what's on the horizon.

Concerns surrounding data privacy originated long before the internet or even computers. The first efforts to legislate the "right to be left alone" came in 1890, with lawyers arguing that all citizens deserved the right of privacy. This need became more urgent a century later, as computers became more mainstream, and the need to protect transmitted data became more urgent. In the mid-1990s, we began to see industry-based compliance regulations put in place, such as HIPAA in healthcare, Sarbanes Oxley Act in financial circles, Payment Card Industry Data Security Standard (PCI DSS) to regulate credit card payments.

Also in the in the 1990s, the EU introduced the European Data Protection Directive, which put the introduced the concept of sensitive personal data. The EU continued to fine-tune its approach to personal data privacy, adding protections for email addresses and mobile phone numbers, and response time for reporting data breaches. The idea of "the right to be forgotten" came in 2014, following a lawsuit against Google to remove information from search results. Finally came the announcement of GDPR in 2016, and its implementation in May 2018. Despite the industry-related compliance, the U.S. has been slow in its development of any consumer data privacy regulations. Members of Congress introduced different legislation over the years to address data protection, but like most bills, no action was taken. The states have been more active but disjointed in their efforts. CCPA, which became live on January 1, 2020, is the best known, but laws in other states including New York, Maryland, and Hawaii have been introduced and are in different phases of the legislative process. Many of these laws discuss similar protections, such as the right to delete, the right to access, and the right correct. They also outline definitions of personally identifiable information (PII) and actions if there was a data breach.

How these compliance regulations will play out in the long run remains to be seen. Organizations and governments are still in a learning curve about enforcement. However, since GDPR went online, organizations have been fined and are facing consequences. More importantly, customers are stepping forward to take control of their personal sensitive data, forcing companies to comply. Those that can't are facing reputational hits and potential loss of business. Without a clear view of what will happen going forward, it is necessary companies take action sooner rather than later to handle data privacy and compliance concerns.

Why You Need Data Privacy and Compliance Software

Most companies already deploy software platforms that manage cyber threats. Traditionally, organizations focused mostly on the risk to the network and the endpoints, and in the past, that focus worked fine. But now, cyber threats are increasingly sophisticated. Cybercriminals want your most valuable asset – your data. At the same time, consumers have been victims of corporate data breaches, and they want businesses to improve on how they manage privacy risks. The intersection of cyber risk and privacy risk is where true data privacy management lies.

The amount of data generated by a single company, however, is too massive to manage by human effort alone. According to IDC Global DataSphere, worldwide data will grow 61 percent to 175 zettabytes by the year 2025, with much of that data stored in the cloud and off premise. Complex compliance regulations add a level of urgency to the ability to properly manage data and ensure minimal data privacy risks. Being in compliance isn't just about ensuring PII is secured, but also about protecting the organization's value and reputation. That's why turning to an automated data privacy platform is necessary. It adds efficiency to the data management process.

With automated tools, organizations can improve on areas such as privacy impact assessments (PIA), data protection impact assessments (DPIA), data mapping/data inventory, and enterprise assessments.

How do you know if deploying data privacy and compliance software is the right option for your company? There are a couple of indicators that include:

- Your current data privacy program isn't keeping you compliant.
- You conduct so many PIAs and DPIAs a year that you need more than a spreadsheet to keep track.
- You have a lot of built-in businesses complexities, such as multiple locations, global clientele, in an industry with multiple compliance regulations to follow, you gather and store massive amounts of PII from customers.
- You struggle to classify your data to make it easier to find and allow a customer the right to be forgotten.
- You don't understand what terms such as Data Subject Access Requests (DSAR) or Subject Right Access Requests (SRAR) mean or how they operate within the different privacy laws.

What Your Data Privacy Software Should Do

Once you decide that your company will benefit from deploying data privacy and compliance software, you next need to understand the options that are out there and what the software will do to improve your data privacy and compliance posture. There are several different data privacy software tiers, including:

- Privacy technology platforms that handle workflow management and data and privacy assessments. This type of software gives you an overview of your company's data and provides a structure to achieve compliance.
- Data discovery systems allow you to find where PII is throughout your network and storage providers, often providing automation in tandem with manual searches.
- Platforms designed to search and manage data subject requests.

The software should be intuitive and compatible with your current software platforms. A system that is easy to use and can easily work with you entire IT network will be more efficient. But you want to go beyond a simple plug-and-play option, but rather have a solution that recognizes what data should be collected, where it is stored, how it is used, and who it belongs to. Compliance software should be up-to-date with the latest laws, recognizing the difference between CCPA, GDPR and HIPAA, for example, and ensure data collection and classification meets each compliance required by industry, federal, state or international law.

Overall, your data privacy and compliance software should be able to complete the following tasks:

- Discover. The software should be able to locate both structured and unstructured data across the network, cloud systems, mobile devices, and all endpoints. Discovery phase gives you a picture of your overall data landscape.
- Classify data. This is one of the most important steps of your privacy and compliance software, and the importance of classifying data will be touched on in greater depth in this paper. In a general overview, your software should be able to provide a basic view of the type of data and its location across your network and endpoints.
- Understand the context of the data. This allows you to best operationalize your data, which will improve productivity and overall business processes. Understanding context ensures that you are using the right data at the right time.
- Control the data. Your software program should allow you to find data quickly and determine that it is the correct data that is stored or destroyed, as well as determine access by other parties.
- Meet compliance. The right software will sort out the confusion behind data privacy regulations, as well as produce Data Subject Access Requests (DSAR) and Subject Rights Request (SRR) request information that demonstrate protection. Classification of data is a vital step in allowing for compliance.
- Platform architecture. The platform should be easy to operate, as well as scalable to provide multiple layers of security. The software should have key integrations with common vendors and should also be able to operate both on-premise and in the cloud.

Beginning with Data Discovery

Every company holds sensitive data. The problem is organizations don't know how much sensitive data, where it is stored, or if it is structured or unstructured. Before you can take any real steps to be in compliance with data privacy laws, you have to be able to locate all of your data and understand your entire data landscape.

Data mining tools will search deep into your databases and storages systems, whether they are onsite or in a data center, investigating all types of files, including images and biometrics. This gives you extensive visibility into your data, allowing you to pinpoint when it was first created and every subsequent step of its lifecycle. Discovery also shows problem areas, alerting you to data at risk.

You can't follow any other protocol of data protection if your data remains hidden. Discovery and the processes behind it is the initial step needed in order to classify data.

The Importance of Classifying Data

Data is every organization's most valuable asset, but it loses its value if you aren't able to utilize it properly for everyday business processes. It takes on added importance when data privacy and compliance is considered. Data classification can better organize collected and stored data, as well as enhance your overall cybersecurity posture.

Data classification places a key identifier on your data and raises awareness to the end user as well as allowing it to be found easily and efficiently. It also ensures the correct handling and monitoring of sensitive data both in and outside of an organization, a critical component to protecting your most valuable data. Here's how classifying your data improves both your business posture and your data privacy protections.

- Compliance. Whatever your industry vertical or location, chances are there will be governing bodies, internal audits and mandates with which your company must comply. Then combine these industry compliances with GDPR, CCPA, and other compliance laws on the horizon, and you have a virtual alphabet soup of regulations to follow. What makes some of these laws so difficult is that none of them follow the same script. For example, while GDPR and CCPA are similar, there are some clear cut differences, such as the size and value of the company determining if the regulations must be followed (for GDPR, it is everyone who does business with a EU citizen, while CCPA only impacts larger companies, and it is undetermined what upcoming laws will require). It feels nearly impossible trying to keep up with all the different requirements to stay compliant with multiple regulations. Data classification allows you to put order to your data and properly prioritize it based on its sensitivity. Consider what data is most important to your company – is it financial records, personal customer data, or a proprietary recipe or other intellectual property? By placing a metadata tag onto each piece of data enables easy identification of your most sensitive assets.
- Improve ROI of existing technologies. Being able to identify your organization's data also helps to improve the performance and achieve greater ROI on expensive security technologies already in place. For example, most companies deploy encryption technology (a GDPR compliance requirement) to ensure that information is protected while in motion or at rest. Adding metadata tags to sensitive content allows you to focus on encrypting the assets that are of most value rather than wasting time protecting the lunch menu or emails reminding employees to come to Karen's birthday party in the break room.
- End user awareness. People are the most powerful tool in any business's security and privacy strategy and empowering them with knowledge is the key to the strategy's success. The seemingly small action of adding visual labels such as headers and footers onto a document or email can raise end user awareness and help them in becoming more security focused and encourage people to 'err' on the side of caution. Similarly, visual labels and watermarks can be applied to data to alert the user to behave more cautiously. Many data leaks are accidental and could be avoided if a data classification solution had been in place to raise user awareness, thereby deterring sensitive content from being stored on a USB or uploaded to third-party web portals and public cloud options. Using visual labels also encourages users to be more responsible and aware when handling physical copies of data that have been printed out. It's safe to say that data classification is central to a well-thought-out security strategy.

What Goes into Classifying Data

Classifying unique data helps your organization allocate its resources and set priorities, meaning you'll be able to take the most-stringent measures to protect the most-sensitive data.

Examples of classification labels are:

Public

Not unique to the organization and not related to internal matters

Internal

Unique to the organization but not for public release, such as internal business procedures

Confidential

Not for distribution, including memos and corporate strategy documents

For example, a Word document containing intellectual property data would be classified as confidential. That classification would be embedded into the document and prominently displayed. Seeing that classification, an end user knows to respect specific rules for the document, such as not to attach it to an email or save it in the cloud.

Automated controls in the software can enforce the same rules by not allowing it to be attached or saved to the cloud and can even destroy a document found in restricted locations. But before any of those actions can take place, the document must be classified, which is why it's essential to put the classification horse before the protection cart.

No matter how you classify your data, there are guidelines of what you should know about the information your company generates and accepts from customers. This includes:

- Know your data's identity- classification schema- icon overlay
- Create user awareness
- Automatically classify data within metadata and alternate data streams
- Persistent classification - fix bad behavior and promote a safe culture
- Minimize Access and shrink the target
- Ensure appropriate level of access to sensitive information
- Determine when data was last accessed
- Assign accountability to data owners
- Ensure unsafe sensitive data is remediated
- Enforce data governance
- Use the classification/tagging/labeling system and taxonomy of your business

Classification happens at throughout all stages of the data lifecycle, from creation to destruction. Data privacy and compliance software will keep track of this lifecycle for each piece of data, knowing when it moves from storage to use to sharing, and will also prevent reduction and additional storage costs. This is important for privacy compliance, as it prevents data from being repeated and hidden throughout the network.

While many businesses have a data classification policy, almost invariably they are manual, and therefore scale poorly and do not integrate with a business's active defenses. A data classification matrix forms the core of a data classification system by matching categories of data (e.g., Proprietary and Sensitive [C-3], Restricted [C-4), etc.) with approved, mandated controls that are to be used globally by the organization.

How Your Data Privacy Software Can Keep You Compliant

Beyond tackling privacy risk and improving the security of your data, a main point of classification – and all other steps of privacy software should accomplish – is to ensure that you remain compliant with laws. To do this your software should be able to complete the following tasks:

Creation of a Data Inventory. A data inventory is a core component of any data protection management program. The inventory represents a system of record that is used for meeting requests for consumer access, correction, and deletion of personal information. It also serves as a go-to reference in the event of a suspected or confirmed data breach. The right technology will identify, remotely or locally, both structured and unstructured personal data throughout your organization in share files, emails, Websites, databases, Microsoft SharePoint, and cloud storage, all with the highest precision.

Privacy program operationalization and management. Privacy program managers need a "command and control" capability if they are to manage the many aspects of their program. A centralized management interface enables privacy team leaders to determine which data is not protected at any given time across the environment, including behind the firewall and on cloud storage. Optimally, it will recognize trends and identify newly created data versus existing data, and which files should be protected.

Breach notification policy and procedures; post-breach "cure" capability. For purposes of complying the any privacy regulations and laws but especially so with CCPA, a business must have a capability to, on demand, mitigate or resolve a breach in a way that "cures" the breach in order to take advantage of the "safe harbor" provisions of the law (California Civil Code §1798.82(a) addresses principle requirements for breach notification for businesses, for example). Key to mitigating or resolving a breach is having policies and procures in place that implement data classification. Data classification is the process of analyzing a document or record and applying a label that indicates who can access it, how it should be protected, how long it should be retained, and how it should be disposed.

Questions to Ask Before Purchasing Data Privacy Software

Congratulations. You've decided that data privacy and compliance software is the right decision for your company. You know you'll need a software platform that offers detailed classification capabilities, compliance protections and the scalability and versatility to work with your current IT architecture.

Before you meet with a sales rep, can you answer the following questions about your data:

- Do you already have a data privacy program in place?
- How well do you know your data, both structured and unstructured?
- What type of endpoints and storage systems do you work with? Have you implemented BYOD programs or have a problem with shadow IT that hinders your data privacy and compliance efforts?
- What compliance regulations must you adhere to?
- What are the driving factors behind your decision to go with data privacy software?

After you narrowed down a few companies from the hundreds of options, questions to ask the sales rep:

- What makes you different from the other companies out there?
- How accurate is your data discovery process?
- How do you approach data classification?
- Where do you look for data? Do you include cloud, on premise, remote locations, images as well as texts, and a variety of endpoints in your search process?
- What does your protection cover?
- How do you help us handle consumer requests to see data or the right to be forgotten?
- What compliance regulations to you cover? Are you prepared for the differences between GDPR and CCPA? Will you provide protection for new laws that may be implemented over the next 12 months?
- How do you fix unprotected or unsafe sensitive information?
- How do you handle remediation if there is a data breach?

Spirion (www.spirion.com) is a pioneer in designing the critical first step of data security and privacy through its data discovery, persistent classification, and behavior software and services.

Since 2006, thousands of organizations across all industries worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs, and reputational damage of successful cyberattacks and regulatory violations. The company was recently ranked by CIOReview magazine as one of the **"20 Most Promising Compliance Technology Solution Providers of 2019,"** an annual listing of 20 companies that are at the forefront of providing compliance technology solutions and transforming businesses. Spirion is an award-winning data privacy software company with recent wins in the Info Security Products Guide 2020 Global Excellence Awards as a Grand Trophy Winner and as a winner in specific categories for SaaS, cloud, and on-premise data discovery and classification.