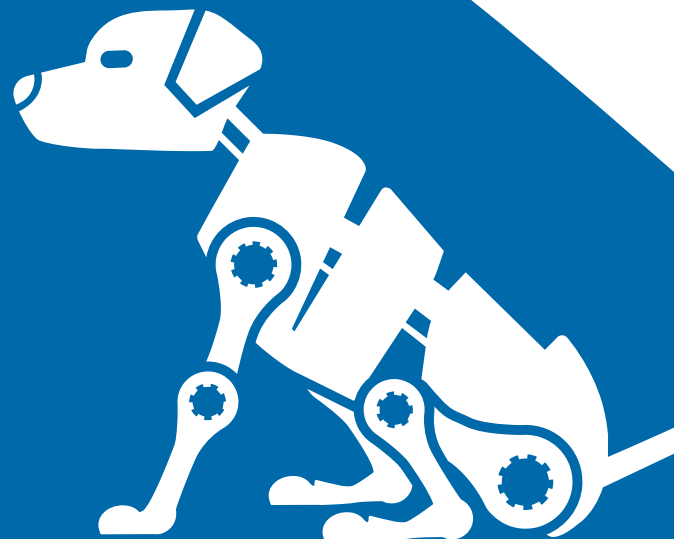


# Using Spirion Sensitive Data Manager™ to Implement the NIST Privacy Framework

A Guide For Data Protection Professionals



# Contents

|  |           |
|--|-----------|
| <b>Why This Guide?</b>                                       | <b>2</b>  |
| <b>New Challenges for Data Protection Professionals</b>      | <b>3</b>  |
| <b>The Introduction of the Cybersecurity Framework</b>       | <b>4</b>  |
| <b>Enter the Privacy Framework</b>                           | <b>5</b>  |
| <b>Problematic data actions and privacy events</b>           | <b>5</b>  |
| <b>The Privacy Risk Assessment</b>                           | <b>6</b>  |
| <b>Making the Framework Easier to Work With</b>              | <b>7</b>  |
| <b>Using Spirion to Implement the NIST Privacy Framework</b> | <b>10</b> |
| <b>Closing Thoughts</b>                                      | <b>12</b> |

## Why This Guide?

“Where do I start?” It’s the most common question posed by data protection professionals tasked with leading a new data privacy management effort. It’s not an easy question to answer and it is especially challenging with modern data protection laws, which can be overwhelming in their scope and usually don’t specify how to comply, only that compliance is mandatory by some date. In fact, it’s not always clear if a given law even applies to a particular organization. This Guide was developed to assist professionals with using Spirion and the NIST Privacy Framework in concert to navigate the often-obscure path to compliance with those laws. As will be explained below, the Framework breaks core privacy functions such as data identification and governance into a collection of sub-functions that will produce particular compliance results or “outcomes.” While these sub-functions have been well designed, they are also very detailed. This Guide will distill those sub-functions into plain English and assist in significantly shortening the path to complying with an array of data protection mandates.

# New Challenges for Data Protection Professionals

Over the past decade, data protection professionals have witnessed a sea of change in the requirements for protecting personal data. Those requirements used to be primarily focused on placing controls on narrow types of data (such as healthcare), with some added legal mandates. Now, data protection laws broadly define what qualifies as personal data (just about anything) and impose many legal and quasi-legal mandates (such as data portability). The result has been a lack of consistency among these requirements, the creation of legal grey areas, and the need for involvement by professionals from outside of information security, such as legal and product management. This has resulted in the need for a generally applicable framework to help delineate privacy issues; it has also resulted in the need for purpose-built technology to drive successful outcomes.

## What precipitated this change?

- **The introduction of new Internet services (social media, Web 2.0) and new technologies (cloud, smart phones, Internet of Things).** Over time, the ability of legal systems in the U.S. and overseas to effectively regulate the processing of personal data eroded, owing to the rapid adoption of social media services such as Facebook and the introduction of new technologies. In particular, the so-called Internet of Things or IoT (Internet-connected devices) has created vulnerabilities that have proven very difficult to remediate.<sup>1</sup>
- **The evolution of the nature of personal data.** Before the Internet and modern telecommunications became significant parts of the global economy, personal data existed primarily in the form of personally identifiable information (PII), which consisted of elements such as Social Security and driver's license numbers, addresses, and phone numbers. This has evolved to include machine-readable data such as IP and MAC addresses, geo-location information, and advertising IDs. Completing this transformation was the addition of "special" or "sensitive" personal data, consisting of elements such as racial and ethnic information, political and religious beliefs, and data concerning health or sexual orientation.
- **A seemingly never-ending litany of data breaches and misuse.** Since the early 2000s, breaches of personal data have occurred with regularity within government and the private sector, and this phenomenon accelerated in the 2010s in spite of near-universal promulgation of breach notification statutes. In recent years, misuse of personal data by businesses has emerged as a distinct problem. A report published early in 2020 by the Norwegian Consumer Council on use of personal data by the advertising technology (or AdTech) industry revealed widespread abuse in the sharing of personal data by popular mobile apps.<sup>2</sup>

---

<sup>1</sup> As of this writing, two class-action lawsuits have been filed against Internet-connected doorbell manufacturer Ring LLC based on alleged weaknesses in the device's security controls. See *LeMay, et al, v. Ring LLC*, 2:20-cv-00074, (Jan. 3, 2020), found at <https://www.classaction.org/media/lemay-et-al-v-ring-llc.pdf> and *Abhi Sheth v. Ring LLC*, 2:20-cv-01538, (Feb. 14, 2020), found at <https://www.courtlistener.com/docket/16860151/sheth-v-ring-llc/>.

<sup>2</sup> *OUT OF CONTROL, How consumers are exploited by the online advertising industry* (January 14, 2020), found at <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>.

The upshot of all of this was the introduction of the EU General Data Protection Regulation (GDPR or Regulation) in April of 2016.<sup>3</sup> The Regulation sought to control how personal data was being used, not merely how it should be protected. In June of 2018, the California legislature passed its analog to the Regulation, the California Consumer Privacy Act of 2018 (CCPA), and then-governor Jerry Brown signed it into law. Since then, a wave of new data protection statutes and regulations have swept across the U.S., and more are on the way.<sup>4</sup>

## The Introduction of the Cybersecurity Framework

One challenge of successfully implementing the GDPR was (and is) that the European Commission did not issue an implementation guide or audit guide by the time the Regulation became enforceable in May of 2018 (and has not issued either to date). As a consequence, implementation teams used privacy principle guidelines such as Generally Accepted Privacy Principles (GAPP) and the OECD Privacy Framework. While these documents have significant value, they were published well in advance of the Regulation and could only assist implementers so far. This lack of documentary assistance is the rule, not the exception, with data privacy and security laws.<sup>5</sup> What was needed was a methodology that could assist in implementing any data protection law and would not be made obsolete by new technologies or services. For the cybersecurity mandates of the GDPR, such a methodology had recently emerged: the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework (or CSF) was introduced in 2014, following the issuance by the Obama administration of Executive Order (E.O.) 13636 in 2013. The CSF rapidly gained acceptance in the private-sector cybersecurity community<sup>7</sup> and in 2017 its use was made mandatory for the federal government.<sup>8</sup> The CSF was designed to address cybersecurity risks within an organization and across its supply chain. It features three components:

- **Framework Core.** The Core represents five distinct and concurrent functions that make up the lifecycle of managing cybersecurity risk: Identify, Protect, Detect, Respond, and Recover. Each function is mapped to several categories, which are then mapped to several subcategories, and finally to reference materials.
- **Framework Profile.** A Profile is a collection of categories and subcategories that will produce particular cybersecurity results or “outcomes,” e.g., identifying hardware and software assets as part of a larger asset management program. Existing Profiles are then compared with target Profiles to determine where gaps lie; from there, organizations will prioritize remediation efforts accordingly.

---

<sup>3</sup> REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>4</sup> See, e.g., *New U.S. State Data Protection Laws Enforceable in 2020* at [https://info.spirion.com/DS2020-Q2-2020EnforcedStateLaws\\_LPRegistration.html](https://info.spirion.com/DS2020-Q2-2020EnforcedStateLaws_LPRegistration.html).

<sup>5</sup> For an example of such a document, see Draft NIST Special Publication 800-171B, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, found at <https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf>.

<sup>6</sup> Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013). See also <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

<sup>7</sup> According to NIST, as of 2015, 30% of U.S. organizations use the CSF; that number is expected to increase to 50% by 2020. See *Cybersecurity Framework*, found at <https://www.nist.gov/industry-impacts/cybersecurity-framework>.

<sup>8</sup> Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017). See also <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

- **Framework Implementation Tiers.** An Implementation Tier is a measure of how risk-informed the implementation of a particular cyber risk measures is, as part of the organization's overall organizational risk management. The four Tiers are: **Partial**, **Risk-Informed**, **Repeatable**, and **Adaptable**. The CSF authors do not consider this to be a maturity model, which tends to focus on effectiveness and repeatability. Rather, the focus is on the dynamism of the risk informed-ness of a particular cyber risk measure.

While the CSF addressed the protection of personal data from the perspective of confidentiality, integrity, and availability (the traditional "CIA Triad"), more was needed to address how personal data was used by businesses, and how it was to be stored, shared (especially with third parties), and retired when no longer useful. Again, NIST provided a needed framework.

## Enter the Privacy Framework

NIST kicked off development of the Privacy Framework (the Framework) in October of 2018 and produced a first draft a year later. Version 1.0 was released in January of 2020.<sup>9</sup> Like the CSF, risk management is the essence of the Framework, and NIST has stated that

**[T]he Privacy Framework's purpose is to help organizations manage privacy risks by:**

- Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicating about their privacy practices; and
- Encouraging cross-organizational workforce collaboration—for example, among executives, legal, and information technology (IT)—through the development of Profiles, selection of Tiers, and achievement of outcomes.<sup>10</sup>

Like the CSF, the Framework features a Core, Profiles, and Tiers. However, the Core is comprised of different functions than that of the CSF: Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P (the "-P" designation is used to distinguish a Framework function from a CSF function).

## Problematic data actions and privacy events

The Framework also features two important concepts, the problematic data action and privacy event:

- **Problematic data action.** A *data action* is a singular data life cycle operation, such collection, use, or sharing of personal data, while *data processing* is a collective set of data actions. A *problematic data action* is one that could cause an adverse effect for individuals.<sup>11</sup> Why not simply call this a threat? According to one NIST analysis, "[t]he NIST privacy engineering model uses the term 'problematic data-action' rather than attempting to expand the 'threat' risk factor to encompass pure privacy concerns."<sup>12</sup>

---

<sup>9</sup> NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, found at [https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework\\_V1.0.pdf](https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf).

<sup>10</sup> *Id.* at 5.

<sup>11</sup> *Id.* at 5.

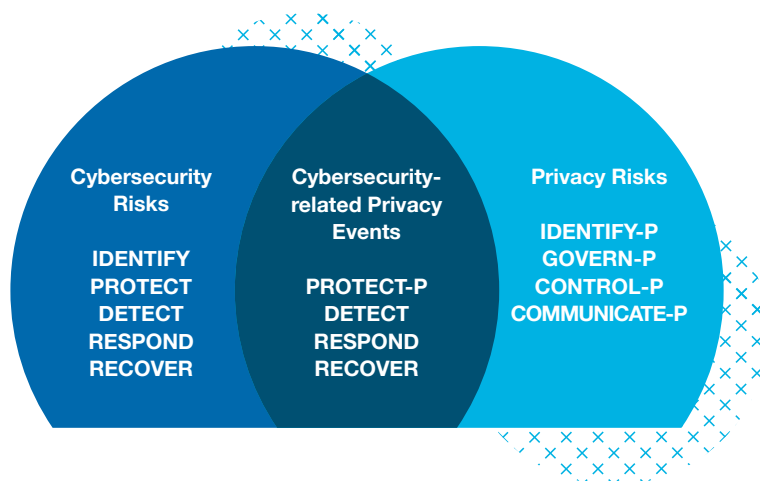
<sup>12</sup> See Summary Analysis of the Responses to the NIST Privacy Framework Request for Information (Feb., 27, 2019), at 9, found at [https://www.nist.gov/system/files/documents/2019/02/27/rfi\\_response\\_analysis\\_privacyframework\\_2.27.19.pdf](https://www.nist.gov/system/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf).

- **Privacy event** A *privacy event* is the occurrence or potential occurrence of problematic data actions. The Framework also describes privacy events as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.<sup>13</sup> This is why the term “breach” is not used – privacy events can encompass many negative actions. However, the Framework does use the phrase “privacy breach” in describing cybersecurity-related privacy events in the Protect-P function.

## The Privacy Risk Assessment

Completing the introduction of the Framework is the idea of a privacy risk assessment. While there are likely many ways to define such a process, NIST defines it as “a sub-process for identifying and evaluating specific privacy risks.”<sup>14</sup> The importance of a properly conducted privacy risk assessment cannot be overstated; it is a reference document that will be used to determine the type and magnitude of resources that will be employed to manage the underlying risk. Many, if not most, data protection laws and regulations either mandate or strongly imply that proper controls be based on the assessment. If a major privacy event (such as a breach) occurs, the assessment will likely be implicated in the resulting litigation or regulatory enforcement action. After completion of the assessment, organizations may choose to mitigate the risk, or to transfer it, avoid it, or accept it. The Framework acknowledges that the “methods for safeguarding these values may differ, and moreover, may be in tension with each other,” and describes how making personal data difficult to access may make control by individuals over their own data difficult as a result.

The Framework’s layout closely resembles that of the CSF by design; while the Framework can be used by itself, it was designed to dovetail with the CSF. One option is to incorporate just the CSF’s Detect, Respond, and Recover Functions, while another is to use all five functions to collectively address privacy and cybersecurity risks.



**Figure 1.** Venn diagram displaying the collaboration between the NIST Cybersecurity and Privacy Frameworks

<sup>13</sup> See *Id.*, n. 9, at 5.

<sup>14</sup> The Art. 29 Working Party (now the European Data Protection Board) describes a data protection impact assessment as “a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.” See Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (Oct. 13, 2017) at 4, found at [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)

# Making the Framework Easier to Work With

At 43 pages, including appendices, the Framework is a bit shorter than the CSF (55 pages) and significantly shorter than the NIST Risk Management Framework (183 pages). However, the Framework's depth can be overwhelming at first glance: Across the five functions are 18 categories and 100 subcategories. Just the first category of the Identify-P function, Inventory and Mapping (ID.IM-P), has eight subcategories, each of which is likely to entail substantial effort. Some, such as ID.IM-P8 (data mapping), likely merit their own projects in order to successfully realize the outcome envisioned by the Framework's authors.

| Function  | Category  | Subcategory  |
|---|---|--|
| <b>IDENTIFY-P (ID-P):</b> Develop the organizational understanding to manage privacy risk for individuals arising from data processing. | <b>Inventory and Mapping (ID.IM-P):</b> Data processing by systems, products, or services is understood and informs the management of privacy risk. | <b>ID.IM-P1:</b> Systems/products/services that process data are inventoried.  |
|   |   | <b>ID.IM-P2:</b> Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. |
|   |   | <b>ID.IM-P3:</b> Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.  |
|   |   | <b>ID.IM-P4:</b> Data actions of the systems/products/services are inventoried.  |
|   |   | <b>ID.IM-P5:</b> The purposes for the data actions are inventoried.  |
|   |   | <b>ID.IM-P6:</b> Data elements within the data actions are inventoried.  |
|   |   | <b>ID.IM-P7:</b> The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).  |
|   |   | <b>ID.IM-P8:</b> Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.  |

**Table 1.** The Inventory and Mapping (ID.IM-P) category of the NIST Privacy Framework's Identify-P function contains eight subcategories, each of which is likely to merit significant effort in order to achieve the desired outcome.

When first employing the Framework as part of a larger privacy risk management process, a useful way to understand the call of the categories is to summarize what they're attempting to accomplish. Inventory and Mapping, e.g., is asking about the "where," "what," "why," and "how" of the personal information you, as an organization, control. The Business Environment category can be summarized as "getting everyone on the right seats on the privacy protection bus." This process can be applied for all categories, then used to summarize the function itself. Identify-P, then, becomes the inventorying of both data and processes, understanding privacy interests, and conducting risk assessments (including DPIAs/PIAs). Indeed, the entire Identify-P function can be summarized as "Know thy sensitive data and know thy self."

| Function   | Category                                  | Summary   |
|--|---|---|
| <b>IDENTIFY-P: "Know thy sensitive data and know thy self."</b><br><br>Inventorying both data and processes, understanding privacy interests, and conducting risk assessments (including DPIAs/PIAs) | Inventory and Mapping                     | The "where," "what," "why," and "how" of the personal information you control |
|  | Business Environment                      | Getting everyone on the right seats on the privacy protection bus             |
|  | Risk Assessment                           | "What could go wrong?"  |
|  | Data Processing Ecosystem Risk Management | Are all of the right risk management pieces in place?                         |

**Table 2.** An effective means to understand the call of the categories of a function is to summarize them, then collectively use them to summarize the category itself. The essence of Identify-P is "Know thy sensitive data and know thy self."

This process of first summarizing categories and then the function itself on the strength of those summaries greatly assists the practitioner in understanding what needs to be done and what team members are the best candidates to assign. Moreover, it highlights the need for participation from departments beyond IT or IT Security: Legal, Product Management, HR, Compliance, etc.

| Function   | Category  | Summary   |
|--|---|---|
| <b>"GOVERN-P: "Do you have what it takes to risk manage?"</b><br><br>Prioritize your risk management activities (policies, legal requirements, calibrating risk tolerance) | Governance Policies, Processes, and Procedures      | Are the rudders in place to steer the privacy protection ship?        |
|  | Risk Management Strategy                            | What's your risk management game plan?                                |
|  | Awareness and Training                              | You won't execute any better than you train                           |
|  | Monitoring and Review                               | Who's minding the privacy protection store?                           |
| <b>CONTROL-P: "Get in the weeds with the processing of personal data."</b><br><br>Implement day-to-day practices to manage privacy risk.                                   | Data Management Policies, Processes, and Procedures | All about governing the data life cycle                               |
|  | Data Processing Management                          | Do you have the proper tools for day-to-day personal data processing? |
|  | Disassociated Processing                            | Every personal data process has to have its limits                    |

Continued on next page



|  |   |  |
|--|---|--|
| <b>COMMUNICATE-P: “Get everyone on the same page.”</b><br><br>Educate the team and data subjects about data processing and associated privacy risks. | Communication Policies, Processes, and Procedures       | It’s all about the transparency                                  |
|  | Data Processing Awareness                               | Is everyone playing from the same sheet of transparency music?   |
| <b>PROTECT-P: “Implement, maintain, and leverage InfoSec.”</b><br><br>Implement safeguards to prevent cyber-security-related privacy events.         | Data Protection Policies, Processes, and Procedures     | Have you covered all of your InfoSec basics?                     |
|  | Identity Management, Authentication, and Access Control | Do you know who has access to personal information?              |
|  | Data Security   | Have you implemented all of the necessary InfoSec tools?         |
|  | Maintenance   | Are you maintaining your InfoSec tools?                          |
|  | Protective Technology                                   | Could you be doing more or doing better with your InfoSec tools? |

**Table 3.** Summaries of the Govern-P, Control-P, Communicate-P, and Protect-P subcategories and functions.




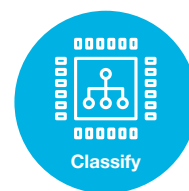
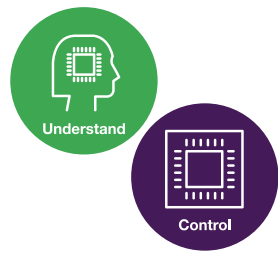

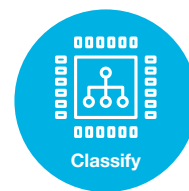
# Using Spirion Sensitive Data Manager™ to Implement the NIST Privacy Framework

When architecting compliance solutions for legal and contractual requirements, data protection leaders are faced with multiple challenges. They must incorporate requirements derived from both U.S. and non-U.S. laws, set up “early warning” mechanisms to detect compliance problems, and be able to document good faith efforts. And all of the forgoing must be risk informed. As a result, leaders require processes that scale, produce consistent results, and function across the enterprise. The only way to achieve those goals is through technology.

Spirion **Sensitive Data Manager™** integrates a data discovery engine, a data classification and marking tool, and an interactive reporting interface into one system. Spirion’s unique technologies offer unparalleled precision in rapidly locating sensitive data throughout the enterprise’s information ecosystem and then automatically protecting or eliminating it. Spirion can customize classification and policy criteria around an organization’s needs, rather than forcing it into a predefined model. Completing this set of capabilities is a single screen for visualization of all sensitive data and associated remediation activities. *In sum, Sensitive Data Manager™ provides data protection leaders command and control over enterprise data privacy operations.*

The capabilities of Spirion’s data discovery and classification technologies address the needs of the NIST Privacy Framework across all functions. Spirion’s Data Privacy Management Framework™ (DPMF) articulates five key areas that data protection leaders should focus on to best advance compliance with a multitude of data privacy laws and contractual demands. Those areas include: **Discover, Classify, Understand, Control, and Comply**. One (or more) of these components will address a given Privacy Framework function, while Comply also represents particular compliance artifacts (such as a DSAR report) as well as the natural – and desired – outcome of an effective approach to data privacy management.

The following table illustrates where the capabilities of Spirion Sensitive Data Manager™ are represented in the DPMF, and how it advances implementation of the NIST Privacy Framework:

| Function   | Implications   | How <i>Spirion Sensitive Data Manager™</i> Advances Implementation  | Spirion <i>Data Privacy Management Framework™</i> Applicability                       |
|--|--|---|---|
| <b>IDENTIFY-P:</b> “Know thy sensitive data and know thy self.”            | The foundation for a data protection program is developing a <i>data inventory</i> , a living directory of where personal data exists in the organization’s information ecosystem. | Spirion’s <b>AnyFind®</b> , <b>Custom Search</b> , and <b>Sensitive Data Definition</b> technologies help build data inventories by identifying personal data throughout your organization in share files, emails, Websites, databases, Microsoft SharePoint, and cloud storage, all with the industry’s highest precision. |    |
| <b>GOVERN-P:</b> “Do you have what it takes to risk manage?”               | Every organization needs a box of governance tools to promote privacy risk management, including policies, processes, plans, and standards.  | Spirion’s industry-leading data <b>Purposeful Classification™</b> technology enables those leaders to “electronify” paper data classification policies, making them living parts of the overall data protection program.  |    |
| <b>CONTROL-P:</b> “Get in the weeds with the processing of personal data.” | Privacy program managers need a “command and control” capability if they are to manage the many aspects of their program.  | <b>Spirion Spyglass™</b> , an interactive reporting interface, provides centralized management for all Spirion functions. Utilizing PowerBI, Spyglass offers a single screen for visualization of all sensitive data and associated remediation activities.   |   |
| <b>COMMUNICATE-P:</b> “Get everyone on the same page.”                     | Transparency of privacy practices, both internally and externally, is an essential element of complying with privacy-centric data protection laws such as the GDPR and CCPA.       | Spirion’s <b>AnyFind®</b> enables rapid, precise location of personal information, improving transparency and advancing compliance with an increasing array of data protection laws.  |  |
| <b>PROTECT-P:</b> “Implement, maintain, and leverage InfoSec.”             | A very common, if not universal, requirement of data protection laws is for the implementation of technical and organizational controls.   | Spirion’s <b>Sensitive Data Watcher™</b> continuously monitors a business’ information ecosystem for new data and when a file is modified, it is instantly searched, automatically classified, and reported upon.   |  |

**Table 4.** How specific capabilities of Spirion’s Sensitive Data Manager™ apply to particular functions of the NIST Privacy Framework via the Spirion DPMF.

# Closing Thoughts

The implementation of modern data protection laws and regulations such as the GDPR and CCPA have become a significant challenge to data protection leaders, owing to the lack of guidance provided by law makers and regulatory bodies. In terms of meeting requirements for protecting the confidentiality, integrity, and availability (the CIA Triad) of personal data, the CSF significantly advances compliance efforts. It does so using a “prioritized, flexible, repeatable, performance-based, and cost-effective approach.”<sup>15</sup> The same is true for the Framework with respect to managing risk associated with the operations conducted on personal data by organizations. This is especially relevant given that the design of the CSF had a strong influence over the Framework’s design, and the latter was designed to work with the former. Part of the charge of E.O. 13636 was to:

**provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks.**<sup>16</sup> (emphasis added)

Likewise, there is an equivalent need in the privacy discipline for products and services to address risks inherent in the processing of personal information. Spirion’s data discovery and classification technologies is a collection of capabilities that meets the standards, methodologies, procedures, and processes developed by the Framework. It does so by uncovering the nature and location of personal data as it exists in an organization’s information ecosystem. This greatly advances the creation and maintenance of the data inventory, both a reference tool and a feeder for privacy functions and roles. It also does so by automatically classifying documents and files containing sensitive data, which in turn empowers allied technologies like data loss prevention and next-generation firewalls to function at their best. In sum, Spirion helps protect what matters most – the sensitive data that is both a responsibility for, and lifeblood of, today’s organization.

---

<sup>15</sup> See *Id.*, n6 at 11741

<sup>16</sup> *Id.*

**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)