

FACT SHEET

nPower[®] Data Classification

An Overview of HaystackID's Enterprise Managed Solutions nPower Program

HAYSTACK[™]



nPower[®] Corporate Compliance Solutions

Using the latest technology, HaystackID's experts empower organizations to categorize, remediate, migrate, and protect their sensitive data. Knowing where all sensitive data resides and how the data is stored and classified is an important compliance requirement. If you don't know the type of PII and sensitive IP data you have and how it's shared, processed, and stored, it is difficult to know if you are complying with privacy regulations and protecting your sensitive IP.

Benefits:

- Ability to demonstrate due diligence and evidence of compliance.
- Improvement of institutional transparency and individual awareness that data management best practices are being followed.
- Improvement of operational efficiencies to minimize the excessive and unnecessary collection, use, retention, and disclosure of personal information and sensitive IP, and perhaps identify simpler and less costly solutions at the start.
- Better protect sensitive corporate IP from unauthorized use or disclosure.

nPower[®] Data Classification

HaystackID will assist an organization to classify data as part of the mapping project. Depending on your requirements, we can build data classification tags according to type, sensitivity, and value. Proper classification helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks. Data classification also helps an organization comply with relevant industry-specific regulatory mandates such as SOX, HIPAA, PCI DSS, and GDPR.

Common data classification:

- **PII:** Non-sensitive PII, Sensitive PII, Non PII
- **GDPR:** Special category personal data, Personal data, Non-personal data
- **HIPAA:** Critical, Restricted, Public
- **ISO 27001:** Confidential, Restricted, Internal use, Public
- **U.S. Government:** Top secret, Secret, Confidential, Sensitive but unclassified, Unclassified

Data classification by sensitivity levels:

- **Restricted:** Disclosure could cause severe harm to individuals and/or the company, including exposure to criminal and civil liability. Has the most stringent legal or regulatory requirements and requires the most prescriptive security controls. Legal and/or compliance regime may require assessment or certification by an external, third party.
- **High:** Disclosure could cause significant harm to individuals and/or the company, including exposure to criminal and civil liability. Usually subject to legal and regulatory requirements due to data that is individually identifiable, highly sensitive, and/or confidential.
- **Moderate:** Disclosure could cause limited harm to individuals and/or the company with some risk of civil liability. It may be subject to contractual agreements or regulatory compliance or is individually identifiable, confidential, and/or proprietary.
- **Low:** Encompasses public information and data for which disclosure poses little to no risk to individuals and/or the company. Anyone can access it without limitation.

GDPR and new state privacy laws require an additional data classification layer for data processing, purpose, and privacy.

- **Data Processing (consent):** New and evolving data privacy regulations require individuals' consent for how organizations use their private data.
- **Purpose (access):** GDPR requires organizations that process EU personal data to clarify the purposes for which they are collecting data. As a result, companies now have to manage their data according to what purpose or purposes it serves within their organizations.
- **Privacy (compliance):** Both GDPR and new US state laws require more advanced data classification schemas.



Conclusion

The mapping and classification of data is critical to understanding the data landscape of your enterprise. By understanding where sensitive data is located across an enterprise, HaystackID can mitigate your data risk footprint. HaystackID's data mapping and classification delivers this insight with a consistent process that identifies and tags all sensitive information in structured and unstructured forms across your enterprise. Together, data mapping, classification, migration, and remediation will make data more secure by providing the critical first step in a comprehensive data privacy and security program.

Learn More. Today.

Contact us today to learn more about how HaystackID's Enterprise Managed Solutions nPower Program can help you manage your enterprise legal data and operational initiatives.

About HaystackID

HaystackID™ is a specialized eDiscovery services firm that helps corporations and law firms securely find, understand, and learn from data when facing complex, data-intensive investigations and litigation. HaystackID mobilizes industry-leading cyber discovery services, enterprise managed solutions, and legal discovery offerings to serve more than 500 of the world's leading corporations and law firms in North America and Europe. Serving nearly half of the Fortune 100, HaystackID is an alternative cyber and legal services provider that combines expertise and technical excellence with a culture of white-glove customer service. In addition to consistently being ranked by Chambers, the company was recently named a worldwide leader in eDiscovery services by IDC MarketScape and a representative vendor in the 2021 Gartner Market Guide for E-Discovery Solutions. For more information about its suite of services, including programs and solutions for unique legal enterprise needs, go to HaystackID.com.

