

# Compliance Solutions For Privacy



Worldwide Public Sector organizations, public companies, regulated industries, and even small-to-midsized businesses may be subject to a range of privacy and information security requirements. Privacy<sup>i</sup> is a major concern of any organization that handles personally identifiable information (PII) or protected health information (PHI). Corporations and government agencies are also concerned with data and information security, charged with the goal of protecting confidential information including corporate trade secrets as well as mergers and acquisition data. This is a very real threat to every company, not just those specializing in PII or PHI. A fundamental tenant of almost all compliance programs is the principle that private or sensitive information must be available only to people that have a right to access it and must be protected from those who do not.

AvePoint Compliance Solutions allow Chief Privacy Officers, Chief Information Security Officers, Compliance Managers, Records Managers, SharePoint administrators and company executives to implement automated access and content controls for their enterprise-wide IT systems (and file share systems) by enabling them to understand how their systems are being used and instill controls to maximize efficiency and access while also helping to prevent breaches from happening. However, if and when a breach does occur, AvePoint Compliance Solutions also enables appropriate personnel to swiftly detect those breaches, track, respond and recover – thereby mitigating the likelihood of a catastrophic incident.

## Key Challenges

Detect	Track and Report	Respond and Resolve	Prevent
Automate a comprehensive assessment to identify content and framework privacy issues	Reports with configurable “risk” levels can be distributed to compliance officers, administrators, and content owners for review and response	Investigate, respond to and resolve compliance issues by prioritizing what to fix first, what to remove, and what issues may require no action at all	Prevent compliance issues through real-time scanning, tagging and action

## AvePoint Compliance Solutions for Privacy

Assess Existing Sites and Content	Report on Compliance Violations	Respond and Resolve PII Violations	Design a Comprehensive Privacy Risk Management Strategy
<ul style="list-style-type: none"> <li>• Generate detailed, granular risk-level reports of content containing privacy and sensitive information with configurable scans for violations out of the box (e.g. PII and PHI) to locate offending content, informing organizations where the majority of non-compliant or content is stored</li> <li>• Determine the nature of existing sensitive data by scanning against pre-configured or customizable test definitions files</li> </ul>	<ul style="list-style-type: none"> <li>• Aggregate Privacy issues with additional “context” about the non-compliant content               <ul style="list-style-type: none"> <li>• What is the nature of the sensitive (or non-compliant) data</li> <li>• Where is it?</li> <li>• How old is it?</li> <li>• Who created it?</li> <li>• Who can access it and who has accessed it?</li> </ul> </li> <li>• Report on the age, update history, and user and content permissions as well as manage individual user or group profile security settings</li> <li>• Track all user and group activity to determine origins of compliance infractions and users who have accessed this content</li> </ul>	<ul style="list-style-type: none"> <li>• Design an information architecture to address privacy requirements for all SharePoint and network content, including existing content and the content transferred in real time</li> <li>• Determine appropriate actions to the at-risk sensitive information based on the privacy requirements of SharePoint or file-based information</li> <li>• Tag and classify PII data to indicate the sensitivity level of that content</li> <li>• Move or restrict permissions as well as automatically notifying appropriate team members to resolve compliance issues</li> <li>• Strictly regulate user-generated content to prevent the creation or upload of sensitive, harmful content</li> </ul>	<ul style="list-style-type: none"> <li>• Determine a best practices and integrated full risk management life cycle approach for redaction and remediation of any identified security compliance issues</li> <li>• Provide user generated or automated metadata (SharePoint or embedded metatags) to classify and protect PII content as it is added to a site</li> <li>• Automatically process and protect privacy information based on pre-defined rules to prevent exposure to users that should not have access to these documents by blocking, quarantining, publishing (with notice), and moving content to the appropriate place or automatically restricting permissions and access to suspect content</li> <li>• Investigate usage patterns and monitor any information to assess the effectiveness of the privacy management strategy</li> </ul>

AvePoint Compliance Solutions helps organizations’ risk and privacy stakeholders scan their environments and granularly assess the compliance situation to the key stakeholders in order to make agile, proactive decisions in addressing non-compliant content – including the ability to tag and classify the non-compliant content by moving it to the appropriate location, quarantine, restructuring the security and permissions, or even deletion.

While this type of vulnerability may sound simple at first glance, looking for these kinds of issues across thousands and/or millions of documents is impossible to do without automation. AvePoint Compliance Solutions creates a true heat map of non-compliant content within your SharePoint environment. It is only with this kind of analysis that true decisions can be made about the level of risk that this content poses.

### Next Steps

If you would like a solution demonstration or receive pricing information, please contact: [ComplianceSolution@AvePoint.com](mailto:ComplianceSolution@AvePoint.com) or your AvePoint sales representative.

<sup>1</sup> AvePoint is a corporate member of the International Association of Privacy Professionals (IAPP)