

Privacy: GDPR, HIPAA, PCI

- **Purpose:** Its purpose is establish compliance to GDPR, HIPAA, PCI and other Privacy-focused standards / regulations / requirements. A privacy program to meet these regulations has become table stakes for operation, no longer optional. The business climate forced by the threat of severe fines and legal complications driving companies to also flow down the same requirements to their partners / suppliers. The entry to business relationships requires that this compliance is documented / validated. SCG has the templates / expertise and years of experience doing this for other companies to develop the privacy compliance program from start to maturity. It starts, once again, with the documents that are foundational. And it then flows to ensuring that the associated policy and processes become inculcated into normal operations. Lastly, is the validation step that involves third party auditors. SCG can provide the guidance, the actual development of the documentation and assist the IT and Security Teams with getting the systems part of the operation into compliance to pass the audits.
- **Level of Effort:** The LOE is determined by a project scope worked out with the client. This is not a small task. Getting an organization to a level of privacy compliance is a large undertaking that requires expert hands to guide the process including getting and keeping alignment and interest with the business leadership. This is typically, dependent on the size and complexity of the organization, a project that can span many months, a year, possibly longer.
- **Owner:** The owner of the deliverables would be at the appropriate C-Level executive; Chief Privacy Officer (if there is one) would be the most direct owner.
- **Key Elements of the Work:**
 - **Analysis:** To determine what are the target compliance requirements / regulations / standards. The effort should be done in a manner that meets all of them, not just one. This starts the planning process to perform scoping the project(s).
 - **Scoping.** This is a critical aspect of the consultancy needed to set expectations. The privacy documentation such as impact assessments, will involve every part of the organization and is a large effort to get all the parts coordinated into a consistent, unified set of policies and processes. But the documentation is the easier part. The more challenging part is system implementation; getting the people, processes and technology to compliance requires roadmaps for how privacy data is processed and controlled. This is the essence of GDPR and the other privacy regulations. There is no shortcut, but there are a myriad number of ways that this effort can go into forever with little to show and scarce finances spent. What you get with SCG is the senior (read experienced) consultant to make the projects successful and the outcomes placing the organization compliant and able to deal with the risks.
 - **Documentation:** This task creates the library of policies and processes adopted by the organization to meet the privacy compliance requirements.
 - **Implementation:** Moving the documentation into actual performance is done in a series of projects working with
- **The Solution Package:** The list of deliverables for this service offering includes:
 - Deliverable 1: Word Document and PowerPoint Executive Summary of the Analysis and Scope to implement the projects
 - Deliverable 2: Library of tailored (to the organization) templates of privacy policy and process documents
 - Deliverable 3: Serve as lead for the organization to guide the various organizational groups to implement the privacy requirements as presented in the policy and process documents.
 - Deliverable 4: Management Progress Reports
 - Deliverable 5: Guide the organization to pass the audits

Features of Privacy

- Analysis of privacy requirements that the organization must follow
- Privacy Documentation in the form of Policies and Processes
- Scope to implement the projects that achieve

Benefits of SD

- Operate the business as required by government privacy regulations
- An internal culture and an operating model for privacy as part of supply chain / partner relations
- A way to baseline and maintain the privacy program
- Readiness to pass audits