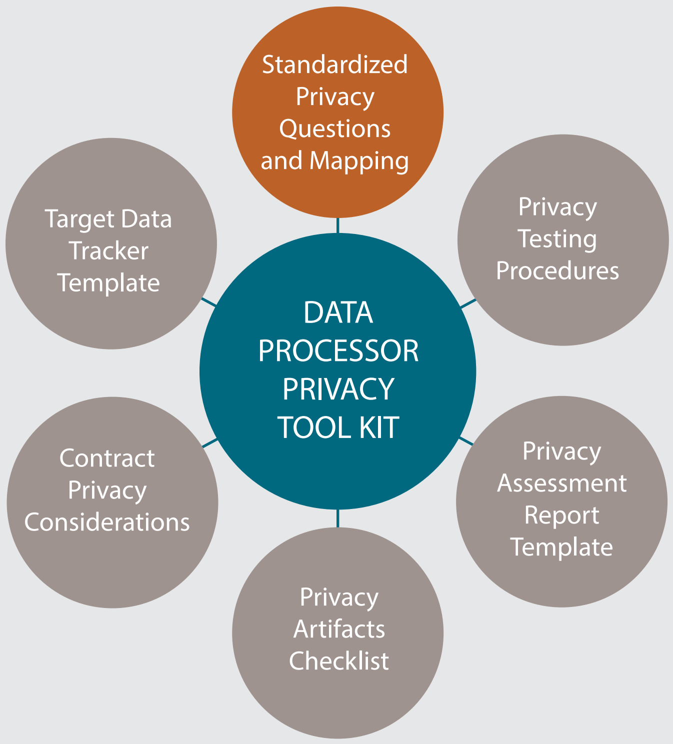
SFG SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING GDPR BEST PRACTICES

GDPR: Data Processor Privacy Tool Kit - Appendix: Shared Assessments Standardized Information Gathering (SIG) Privacy Questions and Mapping



Standardized Privacy Questions and Mapping

Privacy Testing Procedures

Privacy Assessment Report Template

Privacy Artifacts Checklist

Contract Privacy Considerations

Target Data Tracker Template

DATA PROCESSOR PRIVACY TOOL KIT

SHARED ASSESSMENTS

BUILDING GPDR BEST PRACTICES:

GDPR Privacy Tool Kit – Shared Assessments SIG Privacy Questions and Mapping

The Shared Assessments Standardized Information Gathering Questionnaire (SIG) provides its users with a standardized assessment tool, using a robust compilation of questions targeted to gathering pertinent information to determine how risks are managed across a broad spectrum of risk control areas. This Tool Kit includes the SIG Privacy section.

The SIG Privacy Questions and Mapping table is designed to aid organizations in either creating a stand-alone privacy assessment of a third party, or for a third party to respond to a standard privacy assessment. This component has been incorporated into this Tool Kit to assist the industry in adopting streamlined processes for the collection of privacy control information from third parties.

QUESTION RESPONSES

The SIG Privacy section contains a tiered set of questions that allow flexibility for the depth and breadth of the privacy assessment of a third party relationship. The questions are structured with traditional "parent" and "child" questions to enable efficiency in vendor assessments or responses. Parent questions are shown on the table in bold. The section is designed to capture the trigger points that may trigger additional privacy obligations by identifying key privacy controls and potential gaps. A data controller would use these questions to evaluate the privacy posture of a third party relationship, specific to the scope of services. A data processor would use these questions to understand the scope of privacy expectations their client would have in the contractual relationship and in the due diligence or assurance process.

The SIG Privacy Questions and Mapping table includes a Response field for a binary "Yes" or "No" response to indicate whether a control is in place for each question. "Not Applicable" may be used where the data is out of scope of otherwise not pertinent for the service control(s) being examined.

The Maturity field can be used to provide additional dimension to the Response field. The Maturity field can be completed to identify how mature the governance, processes, policies, standards, analyses, tools or procedures are that are under examination. The user can apply their own existing parameters (e.g., High, Medium, Low), or utilize the standardized numeric SIG maturity levels, which are:

1. Not in place, with no plans to implement
2. Partially in place, with no approved plans to implement further
3. Partially in place, with approved plans to implement further
4. In place, with exclusions
5. In place, with no exclusions

The combination of analyzing the Response and Maturity field will provide the most robust review.

The SIG Privacy questions (including the mapping to selected regulations) is provided in this bundle in spreadsheet format, to facilitate the use of the content in the context of the individual user. This spreadsheet can be used to determine what due diligence and/or remediation is appropriate for the service(s) being provided.

SFG SHARED ASSESSMENTS

BUILDING GPDR BEST PRACTICES:

GDPR Privacy Tool Kit – Shared Assessments SIG Privacy Questionnaire

The Privacy Section of the SIG contained in this Tool Kit is based on the physical, administrative and technical safeguards needed from a privacy compliance viewpoint, and does not contain the complete IT controls or information security controls or the full functionality of the complete SIG tool.

For the purposes of the GDPR best practices, we have created the Regulatory Mapping Checklist to focus only on the GDPR privacy obligations. This SIG Privacy Section includes a column that shows the relationship between the SIG Privacy Section questions and GDPR Privacy obligations under the European Union's (EU) General Data Protection Regulation ("GDPR") 2016/679.

To learn more about the more in depth mappings, functionality and content of the complete SIG, please go to: www.sharedassessments.org.

Key privacy frameworks to which Shared Assessments Program Tools are updated include: Generally Accepted Privacy Principles (GAPP); Organization for Economic Co-operation and Development (OECD), US Department of Homeland Security Fair Information Practices Principles (FIPS) and the EU–US Privacy Shield.

Other domestic and international regulations and industry standards to which Shared Assessments regularly aligns, maps and updates its Program Tools include:

- FFIEC – United States' Federal Financial Institutions Examination Council 2015 Cybersecurity Assessment Tool and IT Management Handbook, Appendix A, Revision, May 2015
- FCRA – United States' Fair Credit Reporting Act and key provisions of the Fair and Accurate Credit Transactions Act
- GLBA – United States' Gramm-Leach-Bliley, also known as the Financial Modernization Act of 1999
- ISO – International Organization for Standardization and the International Electrotechnical Commission under the joint ISO and IEC subcommittee - ISO/IEC 27001:2013
- HIPAA – United States' Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104-191, 110 Stat. 1936, enacted August 21, 1996) and the corresponding amendments for business associates under the Health Information Technology for Economic and Clinical Health Act (HITECH)
- PIPEDA – Office of the Privacy Commission of Canada, Personal Information Protection and Electronic Documents Act, 2004

SFG

SHARED
ASSESSMENTS

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted source in third party risk assurance, is a member-driven, industry-standard body with tools and best practices, that injects speed, consistency, efficiency and cost savings into the control assessment process. Shared Assessments Program members work together to build and disseminate best practices, building resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments.

P: (505) 466-6434
F: (505) 466-3111
E: info@santa-fe-group.com