SecureTrust™
a Trustwave® division

SecureTrust™ GDPR Services

PRIVACY INFORMATION SECURITY RISK ASSESSMENT FOR THE GENERAL DATA PROTECTION REGULATION

Benefits

A Structured Risk-Based Approach

- Informed by SecureTrust compliance and security expertise
- Structured plan to prioritize areas of high risk and build a compliance monitoring program

Comprehensive Analysis

- Examination of business strategy, scope and risk appetite
- Investigation of all identified data flows that contain personal data
- Evaluation of operational environment, processes and documentation
- Consideration of processors in the supply chain

Strategic planning

- Risk treatment and recommended risk mitigation solutions
- Helps to incorporate privacy by design into planning
- Additional security control recommendations

The European Union (EU) General Data Protection Regulation (GDPR) requires entities around the world to follow requirements for lifecycle management of personal data, timely incident response, privacy by design and other controls.

The GDPR is a far-reaching regulation that is having a global impact. Enterprises across the globe are subject to rules and penalties for data protection and customer information privacy. Operations must adhere to the GDPR for all processes that handle privacy data which could be used to identify a data subject who resides within the European Economic Community. A comprehensive, organization-wide assessment is an essential early step to accurately evaluate your practices and position your organization to provide data protection, customer privacy and comply with the GDPR.

SecureTrust GDPR Services help your organization prepare and adhere to the GDPR and realize effective data management. SecureTrust services are informed by our long history with security, compliance and data management. For nearly 25 years, SecureTrust has supported information systems communities with world-class guidance on privacy, information security and compliance. And, all SecureTrust professional services are administered with our proven methodology and backed by our proprietary technology, the Compliance Manager application, to track and manage the assessment.

Services are designed to help you determine where your organization should concentrate your data protection efforts. Subsequently, we seek to provide assistance in remediating known issues. And, as your implementation moves forward, we can help gauge your progress toward your objectives.

SecureTrust GDPR Services

SecureTrust GDPR and privacy services help you assess how well you are meeting GDPR requirements and help you create a strategic plan for improving your organizations data protection practices. Services include:

Privacy Workshop

- Helps you understand the scope of privacy regulations, specifically the GDPR and requirements
- Helps plan risk assessment and risk treatment for the protection of personal data
- Helps facilitate senior management endorsement to prepare for compliance with privacy regulation

Privacy Gap

- Helps you identify and assess gaps for the protection of personal data and compliance with regulation
- Helps you remediate and treat Gaps identified during the assessment
- Helps you to amend policy and procedures to ensure effective control of privacy data

Privacy Information Security Risk Assessment

- Provides an assessment of relevant controls and policies used to identify, measure, monitor and control compliance risk
- Helps you identify and assess risks for the protection of personal data and compliance with regulation
- Helps you develop a strategic plan for treating risks to the privacy of personal data with guidelines to reduce or mitigate inherent risk

Privacy Impact Assessment

- Helps you address critical or high-risk processes as required by the GDPR
- Helps you evaluate ongoing compliance and risk for critical and high-risk processes

Privacy Assessment

Privacy by Design

Privacy by design is an important concept for GDPR compliance. It means that each new service or business process that includes personal data must build protection of that data into the design through the entire data lifecycle. A core principle of privacy by design is that it prevents data privacy infractions before they occur. As part of the SecureTrust P-ISRA, we will help you identify to what degree privacy by design is incorporated within your organization.

The SecureTrust P-ISRA will review business processes, procedures and controls against the GDPR requirements including:

- Data breach reporting
- Data security (encryption, pseudonyms, anonymization)
- Data recovery
- Security testing
- Data access rights of natural persons

The SecureTrust P-ISRA will help you identify, assess and treat risk providing recommendations for remediation where necessary. We will review whether responsibilities and accountability for maintaining the protection of personal data are formally documented, communicated and recognized (this includes the third-party partnerships).

We will evaluate the security best practices and procedures that are in place to meet the requirements of the GDPR. We will help you identify critical and high risks where your organization may need to conduct privacy impact assessments as well as help you execute that task. And, together with your organization, we will determine whether procedures in place are sufficient to meet the needs of the GDPR and whether they are in line with your organizations risk management strategy.

Engaging Teams in Your Organization

Compliance with the GDPR involves understanding the scope of personal data in all its forms and how it flows through your entire organization. Many departments must be engaged, including:

- Privacy and Security Governance
- Information Technology
- Enterprise Risk Management
- Legal and Compliance
- Procurement
- Human Resources
- Facilities
- Customer Service
- Finance
- Third-party partners with access to personal data, and more

Assessment Methodology

SecureTrust employs industry standards and general concepts specified in the ISO/IEC 31000, NIST SP 800-39 and NIST SP 800-122 for our P-ISRA and related privacy services. The proposed methodology is data privacy focused and not solely meant to conform to a single standard. Other standards may be used to facilitate the assessment, determined by the size, complexity and needs of your organization.

Additional Privacy Assessments

Privacy Workshop

Many organizations like to participate in a Privacy Workshop prior to the risk assessment. The Privacy Workshop helps members of your organization understand the scope of the GDPR, plan risk assessment, risk treatment and expedites senior management support for investment to comply with privacy regulation and protect personal data.

Privacy Impact Assessment

The SecureTrust Privacy Impact Assessment helps you evaluate ongoing compliance with the high-risk processes identified in the GDPR Privacy and Information Security Risk Assessment. This ongoing monitoring of high-risk processes is required by GDPR.

For more information, visit https://securetrust.com/challenges/by-mandate/gdpr-compliance/.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com