

Service Description

Data Privacy Workshop

Contents

Privacy Workshop	3
SERVICE DESCRIPTION	3
BASE SERVICE FEATURES.....	3
SecureTrust Portal.....	3
Global Compliance & Risk Services	3
DELIVERY AND IMPLEMENTATION.....	3
Project Initiation	3
Phase I: Workshop, Organizational Review and Discovery	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES.....	4

Data Privacy Workshop

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Workshop is a professional services engagement. The Data Privacy Workshop helps identify, assess and plan any gap treatment for the protection of personal data captured, stored or maintained throughout business processes. The Data Privacy Workshop helps facilitate senior management endorsement and cross-functional collaboration to plan and prepare for compliance with privacy regulation.

BASE SERVICE FEATURES

SecureTrust's Data Privacy Workshop service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

Global Compliance & Risk Services

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Security Consultant – An information security consultant serves as the primary resource to deliver the Data Privacy Workshop to assist Client regarding how privacy data is captured, stored, maintained and protected.

Managing Consultant (MC) – An MC provides guidance, project oversight and reporting quality assurance to the Security Consultant and serves Client as a secondary point of contact for escalations and queries.

Data Privacy Workshop – An on-site workshop with interactive question and answer sessions, with all personnel involved in handling personal data and processes with high risk to data subjects focusing on processing activities across the organization.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the service which includes scheduling and conducting the remote kickoff meeting to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, resource requirements and escalation procedures.

Key activities in the Project Initiation phase are:

- Scheduling the workshop date, timing and location;
- Identification of key Client personnel required to facilitate the workshop; and
- Engagement with senior management representatives to understand expectations.

Phase I: Workshop, Organizational Review and Discovery

SecureTrust will work with Client to identify relevant business environments, procedures, processes, systems, and controls which should be considered during the finite duration of the engagement.

Key activities will include:

- Delivery of a workshop presentation focusing on privacy regulation specific to organizational requirements
- Education for Client to achieve understanding of the privacy regulation requirements
- Engagement with key management to understand the business strategy, objective, scope and risk appetite
- Discussion and question and answer sessions for how personal data is captured, stored, maintained and protected on physical and logical media, with consideration of the following:
 - Business goals and strategic directions that impact the handling of personal data
 - Business operations including internally performed and outsourced processes
 - Key IT systems and their security
 - Data flows which may contain personal data
 - Processes and documentation for all controls ensuring the confidentiality and integrity of personal data
 - Roles of Controllers and processors used to process personal data
 - Data protection officer (DPO) requirements and responsibilities
 - Privacy notices
 - Data Transfer outside of the European Union (EU) if applicable
 - Legal basis for data capture
 - Documentation needed to meet privacy regulation requirements
- Identify gaps verbally with potential recommendations
- End the workshop with a close out meeting, summarizing gaps and potential next steps

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with Client.
- Establish communication and escalation plans.
- Create a Client account in the SecureTrust Portal.
- Define high-level project plan consisting of milestone dates, key steps, estimates for duration and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Provide an executive summary report.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan consisting of milestone dates, key steps, estimates for duration and resource requirements.
- Establish communication and escalation plans.
- Accurately provide all necessary information including key stakeholders, applicable Client environment information and configuration requirements.
- Inform SecureTrust of all Client environment maintenance activity and changes that may impact the workshop.

- Accurately respond to requests from SecureTrust teams when establishing contact and collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available Client resources capable of participating in workshop activities.
- Participate in and understand materials explained during the workshop.
- Client acknowledges:
 - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
 - Personnel from the following departments are generally involved:
 - Privacy and Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, Sales, Marketing, Operations and Finance
 - The workshop complements and does not replace Client internal gap and/or risk assessment process.
 - The engagement consists of both remote and onsite assessment activities.
 - SecureTrust will perform the service in the English language.
 - SecureTrust will not create or modify Client documentation as part of the Data Privacy Workshop.
 - SecureTrust will not provide remediation services as part of the Data Privacy Workshop.
 - SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Workshop does not guarantee compliance with data privacy regulation. Client is responsible for making all management decisions with regard to its data privacy policies.
 - The quality and accuracy of the service is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.