SecureTrust
a Trustwave division

Service Description

Subject Rights Request (SRR) Consulting

Contents

Subject Rights Request (SRR) Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Subject Rights Request (SRR) Consulting is a professional services engagement. SRR Consulting is designed to facilitate the process of responding to subject rights requests. The SRR Consulting service provides guidance for data privacy SRR processes and provides recommendations for adherence with privacy regulations or data privacy management programs.

BASE SERVICE 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 and Risk Services (GCRS)

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

Security Consultant – An information security consultant is the primary resource for the fulfilment of the service, responsible for conducting subject rights request consulting activities and reporting.

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.

Subject Rights Request Consulting – Consulting to facilitate the process of responding to requests from a consumer, resident, or subject who has rights pursuant to a privacy law or regulation. SecureTrust will provide guidance for SRR processes and provide recommendations for adherence with privacy regulations or data privacy management programs. SecureTrust will provide a high-level summary report to describe the process and outcomes of the SRR Consulting activities.

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, deliverables, resource requirements and escalation procedures.

Project Initiation activities include:

- Introduction to the Compliance Manager application for data sharing.

Outputs of the Project Initiation phase includes:

- Agreement on the high-level project plan.
- Regular project status meetings with key stakeholders.

Phase I: Discovery

SecureTrust will interview appropriate personnel, including third parties as required, to understand the details of the organization's people, process and technology, regulatory requirements and data privacy management program.

During the Discovery phase, SecureTrust's consultants will collect information from personnel in different levels of the organization as well as from those with business and information technology expertise.

Each interview requires a peer-level group of participants from a corporate level and features a series of collaborative activities. The format of all interviews is the same for each process, but the audience differs to include senior management, operational area management and other staff both business and information technology personnel.

Key activities include:

- Schedule a site visit and\or remote workshop to identify required documentation.
- Identify processes related to an SRR.
- Collect policies, data mappings, and supporting documentation for Client to respond to an SRR.

Phase II: Subject Rights Request Consulting

SecureTrust will work with Client, through interviews, discussions and documentation review to conduct SRR Consulting activities.

Key activities include:

- Assist the Client to identify the processes necessary to comply with an SSR generated from a privacy law or regulation.
- Review the Client's current processes regarding SSR fulfillment.
- Provide Client recommendations to adhere to regulatory requirements regarding SSR fulfillment.
- Assist Client in identifying additional processes, technologies, or solutions to respond and manage SRR.

Outputs of the SRR Consulting include:

- SRR Process flow.

Phase III: Reporting

SecureTrust will create, prepare, and deliver to Client a report documenting findings and recommendations from the SRR Consulting activity to establish a high-level data mapping of scoped and identified PII interactions.

Outputs include:

- Summary report to describe process and outcome of the SRR Consulting activities.

SecureTrust will conduct a closeout meeting with Client.

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, deliverables, and resource requirements and escalation procedures.
- Schedule and conduct kickoff, periodic status and closeout meetings.

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, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable environment information and configuration requirements.
- Inform SecureTrust of all environment maintenance activity and changes that may impact the service.
- 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 resources capable of participating in consulting activities in relation to Client's environment.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
    - Personnel from the following departments are generally involved:
        - Operations, Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
        - Third party data brokers, controllers or processors are involved.
    - The consulting engagement consists of remote and/or onsite activities.
    - The consulting engagement period start and end dates will be determined during the kickoff call.
    - SecureTrust is not responsible for defining systems in scope or whether information provided by Client is accurate.
    - SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the service.
    - SecureTrust will not provide remediation services as part of the SRR Consulting.
    - SecureTrust will not offer any legal guidance or counseling. The provision of SRR Consulting Service 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.