SecureTrust
a Trustwave division

Service Description

Data Privacy Impact Assessment

Contents

Data Privacy Impact Assessment

SecureTrust™ is a division of SecureTrust Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Impact Assessment (DPIA) is a professional services engagement. It is designed to analyze how an entity collects, uses, shares, and maintains personally identifiable information, related to existing risks. The DPIA helps address critical or high-risk processes in accordance with privacy regulations.

BASE SERVICE FEATURES

SecureTrust's DPIA 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 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 serves as the primary resource to deliver the service and assist Client in remediation planning regarding how personal 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.

DPIA – An assessment to address key gaps and processes with high risk to data subjects, focusing on processing activities across the organization including physical and technical control. A SecureTrust security consultant works with Client resources to carry out a comprehensive assessment and produce an actionable report documenting observations and recommendations from the assessment.

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 escalation procedures.

Project Initiation tasks include:

- Identification of key controller and processor personnel required to facilitate the assessment.
- Issuing list of requested documents and meetings to understand the scope of the engagement.

SecureTrust will work with Client to identify relevant business environments, procedures, processes, systems, and controls which should be assessed during the assessment.

Outputs of Project Initiation activity includes:

- Agreement on the project scope and expected deliverables.
- Regular project status meetings with key stakeholders.
- Agreement on project plan, key steps, assessment dates, stakeholders as well as roles and responsibilities.

Phase I: Organizational Review and Discovery

SecureTrust will work with Client and their processors, if applicable, to identify relevant business environments, procedures, processes, systems, and controls which should be considered during the finite duration of the engagement. Only previously identified key gaps and processes with high risk to data subjects will be considered during the engagement.

Key activities include:

- Understand and document the nature, scope, context and purposes of the processing.
- Include data processors, if applicable, to understand and document their processing activities.
- Review the DPIA policy.
- Review of risk assessment, DPIA or project terms of reference.
- Review mitigation action on previous risk assessment or DPIA outcome if applicable.
- Begin an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- Record the outcome of the DPIA, including any difference of opinion with the SecureTrust consultant.

Phase II: Assessment

SecureTrust will conduct an on-site assessment with all personnel involved in critical processes within the scope of the assessment to address key gaps and processes with high risk to data subjects, focusing on processing activities across the organization and including physical and technical control.

Key activities will include:

- Consider the nature, scope, context and purposes of the processing.
- Continue objective assessment of the likelihood and severity of any risks to individuals' rights and interests to include:
    - 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;
    - Processes and documentation for all controls ensuring the confidentiality and integrity of personal data;
    - Roles of controllers and processors;
    - Privacy notices;
    - Data Transfer outside of the EU if applicable;
    - Legal basis for data capture; and
    - Documentation needed to meet privacy regulation requirements.

- Identify measures that can be put in place to eliminate or reduce high risks.

Phase III: Reporting

SecureTrust will create, prepare and deliver a report to Client, documenting findings and recommendations from the assessment to establish a record of the DPIA including the potential likelihood and severity of any risks to individuals' rights and interests.

The following documents and content will be included in the final deliverables:

- A formal DPIA report to:
  - Document the nature, scope, context and purposes of the processing.
  - Record the outcome of the DPIA, including any difference of opinion with individuals consulted.
  - Identify measures, high priority risks and mitigation recommendations.
  - Recommend solutions and specific security controls.

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.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Validate scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine data privacy impact assessment results.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan consisting of milestones 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 assessment.
- Accurately respond to requests from SecureTrust teams when establishing contact and collecting assessment information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.

- Report any processing that is likely to result in high risk to individuals' rights and interests within Client's organization which cannot be mitigated.
- Client acknowledges:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - Personnel from the following departments or third parties are generally involved:
        - Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance. And, controllers and processors.
    - The service complements and does not replace the Client internal gap, and/or risk assessment process.
    - The service is intended for new processes, business lines, products, or services being launched for which a DPIA has not been performed.
    - The service requires that a risk assessment be conducted before the DPIA.
    - The service consists of both remote and onsite assessment activities.
    - The assessment period start and end dates will be determined during the kickoff call.
    - SecureTrust may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
    - 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 assessment.
    - SecureTrust will perform the service in the English language.
    - SecureTrust will not create or modify Client documentation as part of the Data Privacy Impact Assessment.
    - Trustwave will not provide remediation services as part of the Data Privacy Impact Assessment.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Impact Assessment 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.