SecureTrust
a Trustwave division

# Service Description

## Data Privacy Impact Assessment

# Contents

# Data Privacy Impact Assessment (DPIA)

SecureTrust™ is a division of Trustwave Holdings, Inc.

## SERVICE DESCRIPTION

SecureTrust's Data Privacy Impact Assessment (the "Service") is designed to help identify risks to personally identifiable information ("PII") or personal data in accordance with privacy regulatory requirements or data privacy management programs as specified in the applicable Order Form or SOW ("Privacy Requirements"), and will focus only on one specific product, service or process.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between SecureTrust and Client.

## BASE SERVICE FEATURES

The Service includes the following standard features:

### SecureTrust Portal

The SecureTrust Portal features consist of, among others, 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 – A Security Consultant is the primary resource for the fulfilment of the Service, responsible for conducting the assessment, reporting, and consulting activities.

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

DPIA – The Service helps identify risks to PII or personal data in accordance with Privacy Requirements . A SecureTrust Security Consultant will work with Client resources to conduct the Service and will focus only on one specific product, service or process. SecureTrust will produce a final report documenting observations and recommendations from the Service.

## DELIVERY AND IMPLEMENTATION

### Project Initiation

The SecureTrust GCRS team facilitates 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.

## Phase I: Information Gathering

SecureTrust and Client will work together to gather and analyze information on Client's environment.

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 Service. Only previously identified processes with high risk to data subjects will be considered during the Service.

Key activities include:

- Understand and document the nature, scope, context and purposes of Client's data processing activities.
- Review data brokers, controllers, or processors, if applicable, to understand and document their processing activities.
- Review the DPIA policy.
- Review the risk assessment, DPIA or project terms of reference.
- Review mitigation action after previous risk assessment or DPIA, if applicable.

## Phase II: Data Privacy Impact Assessment

SecureTrust and Client will work together, through documentation review, interviews, discussions, facilities inspections, and controls analysis to conduct the Service.

Key activities include:

- Consider the nature, scope, context and purposes of Client's data processing activities.
- Determination of the likelihood and severity of risks to personally identifiable information (PII) 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.
    - Privacy notices.
    - Legal basis for data capture; and
    - Evaluation of risk associated with applicable Privacy Requirements.

## Phase III: Reporting

SecureTrust will develop a draft report documenting observations and recommendations from the Service to establish a record of the potential likelihood and severity of risks to PII.

A draft of the report will be sent to Client for review. Client may comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report.

SecureTrust will provide a final deliverable as defined below:

- Final report to:
    - Document the nature, scope, context, and purposes of Client's data processing activities.
    - Describe process and outcome of the Service
    - Identify measures that Client may put in place to help eliminate or reduce high risks.
    - Recommend solutions and specific security controls.

SecureTrust will conduct a closeout meeting with Client.

## SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from 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 Service.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine the results of the Service.
- Provide Client with information on observations that require remediation.
- Produce a draft report.
- Deliver to Client a final report documenting observations and recommendations from the Service.

## CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- Establish contact and remain available for communications from 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 the Service 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 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 Controllers or Processors are involved.
        - Privacy Officer or Data Protection Officer
    - The Service complements and does not replace Client's internal gap, and/or risk assessment process.
    - The Service requires that a risk assessment be conducted before the Service begins.
    - The Service may consist of both remote and onsite activities.
    - The project 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 Service.
    - SecureTrust will not create or modify Client documentation as part of the Services.
    - SecureTrust will not provide remediation services as part of the Service.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the Services does not guarantee compliance with Privacy Requirements. 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.