# Service Description

National Institute of Standards and Technology

Data Privacy Impact Assessment

Copyright © 2020 SecureTrust, Inc. All rights reserved.

# Contents

**National Institute of Standard and Technology (NIST) Data Privacy Impact Assessment (DPIA)..... 3**

Service Description ..... 3
Base Service Features ..... 3
SecureTrust Portal ..... 3
Global Compliance and Risk Services (GCRS) ..... 3
Delivery and Implementation ..... 3
Project Initiation ..... 3
Phase I: Discovery ..... 4
Phase II: Data Privacy Impact Assessment ..... 5
Phase III: Reporting ..... 5
SECURETRUST RESPONSIBILITIES ..... 5
CLIENT RESPONSIBILITIES ..... 6

Copyright © 2020 SecureTrust, Inc. All rights reserved.

# National Institute of Standard and Technology (NIST) Data Privacy Impact Assessment (DPIA)

SecureTrust™ is a division of Trustwave Holdings, Inc.

## SERVICE DESCRIPTION

SecureTrust's National Institute of Standards and Technology (NIST) Data Privacy Impact Assessment (DPIA) is a professional services engagement. The NIST DPIA identifies risks to personally identifiable information (PII) or personal data in accordance with privacy regulations or data privacy management programs, focused only on one specific product, service or process.

## BASE SERVICE FEATURES

SecureTrust's NIST DPIA 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 is the primary resource for the fulfilment of the service, responsible for conducting the assessment, reporting and assisting Client in remediation planning.

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.

NIST DPIA – An assessment to identify risks to PII or personal data in accordance with privacy regulations or data privacy management programs. A SecureTrust Security Consultant will work with Client to conduct a data privacy impact assessment focused only on one specific product, service or process. SecureTrust will produce a data privacy impact assessment report documenting findings and recommendations.

## 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

Copyright © 2020 SecureTrust, Inc. All rights reserved.

milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures.

Project initiation activities include:

- Introduction to the Compliance Manager application for managing the assessment and/or data sharing.

Outputs of project initiation activity includes:

- Agreement on the high-level project plan
- Commitment to 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.

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. SecureTrust will also collect policies and procedures, data mappings, diagrams and other related documentation to identify the risk profile of people, processes and technologies regarding the risks to PII.

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 include senior management, operational area management and other business and information technology personnel.

Key activities include:

- Schedule a site visit or remote workshop to identify required documentation.
- Engage with key management to understand Client's strategy, objective, scope and risk appetite that impact the handling of PII or personal data.
- Review and understand the applicable privacy regulatory requirements and data privacy management programs.
- Review diagrams, data flows, policies and supporting documentation.
- Review business operations including internally performed and outsourced processes that handle PII or personal data.
- Review key IT systems data privacy related documentation and/or configurations.
- Include data brokers, controllers or processors if applicable, to understand and document their processing activities.
- Review the DPIA policy.
- Review previous risk assessment or DPIA, if applicable.
- Review mitigation action on previous risk assessment or DPIA outcome, if applicable.

Copyright © 2020 SecureTrust, Inc. All rights reserved.

## Phase II: Data Privacy Impact Assessment

SecureTrust will work with Client, through interviews, discussions, and document reviews to conduct a data privacy impact assessment. The impact assessment process will identify risks to the protection of PII and adherence with privacy laws and regulations and/or data privacy management programs.

Key activities include:

- Conduct remote meetings and onsite visits to facilitate interviews, discussions and documentation review.
- Review and analyze data actions on PII or personal data.
- Review and analyze IT system data privacy related capabilities.
- Review and analyze data privacy mappings.
- Confirm the critical assets including people, process and technology handling privacy data.
- Catalog and analyze data actions on PII or personal data.
- Determine the risks to the protection of PII or personal data and compliance with privacy laws and regulations and/or data privacy management program.
- Assign risk values to all risks identified.
- Document the risk assessment results.

Outputs include:

- A documented risk register.

## 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 potential risk to PII or personal data and the data process.

Outputs include:

- Data Privacy Impact Assessment (DPIA) report to:
    - Summarize the risk analysis.
    - Document risks identified by SecureTrust.
    - Provide recommendations to mitigate risk.

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.

Copyright © 2020 SecureTrust, Inc. All rights reserved.

- Schedule and conduct kickoff, periodic status and closeout meetings.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine DPIA results.
- Create, prepare and deliver to Client a final report documenting 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 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 privacy impact assessment 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:
    - 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 brokers, controllers or processors.
        - Privacy Officer or Data Protection Officer.
    - The service complements and does not replace the Client's ongoing internal data privacy risk assessment processes.
    - The service assumes that Client has conducted a risk assessment before the NIST DPIA.
    - The assessment consists of remote and onsite 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 will perform the service in the English language.
    - 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 not create or modify Client documentation as part of the NIST DPIA.
    - SecureTrust will not provide remediation services as part of the NIST DPIA.

Copyright © 2020 SecureTrust, Inc. All rights reserved.

- SecureTrust will not offer any legal guidance or counseling. The provision of NIST DPIA 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.

Copyright © 2020 SecureTrust, Inc. All rights reserved.