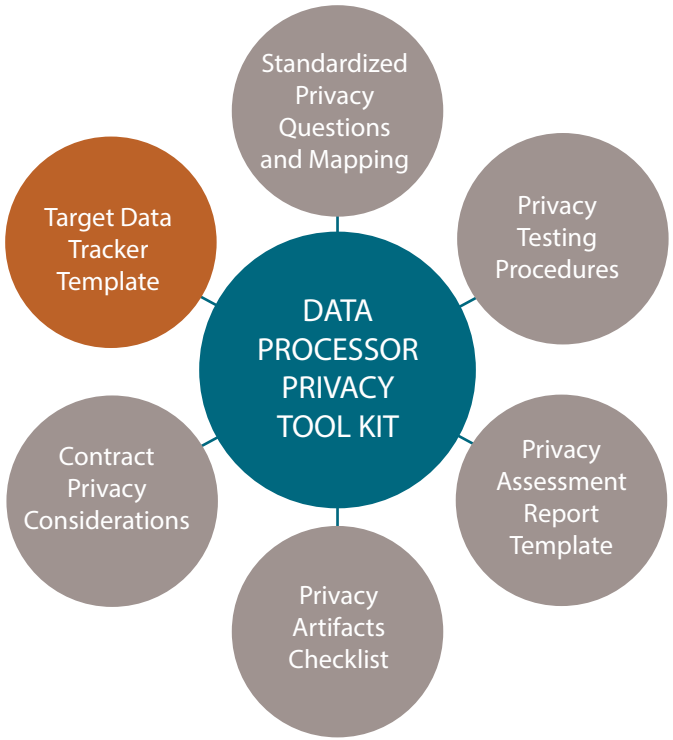
SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING GDPR BEST PRACTICES

GDPR: Data Processor Privacy Tool Kit – Appendix:
Shared Assessments Target Data Tracker



SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR Privacy Tool Kit – Target Data Tracker

The Shared Assessments Program updated its Target Data Tracker (TDT) third party risk due diligence template for the tracking of target data to address the broader third party and data transfer obligations driven by privacy regulations like GDPR.

The TDT is a companion tool to the due diligence process for efficient third party risk assessments. Controllers should address all three areas of concern (target data type, location, sharing) in the table for each third party processor with which the controller engages.

The user may include more granular categories or sub-categories in their own variant of this matrix. While the TDT is *not* designed to be the primary tool for data controllers or processors to conduct their internal data inventory or maps required by data protection authorities; the TDT *is* a template that can be utilized by controllers to summarize the results of risk assessments specific to a set of products or services that are used in the third party assurance or due diligence process. controllers may require a processor (or other third party) to complete a Target Data Tracker in advance of a conducting a more in-depth privacy assessment.

In addition, a processor can proactively maintain a Target Data Tracker for a particular service, to streamline the requests from clients on data inventories, maps or data flows.

The TDT can generally be completed in a matter of hours.

SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR Privacy Tool Kit – Target Data Tracker

Focus: Tracking Data Types, Locations and Third Parties - The TDT streamlines the collection and delivery of summary information about data inventories and data flows in the due diligence process required under multiple privacy or data protection regulations.

Description: The purpose of the Target Data Tracker (TDT) is to address the six critical questions that controllers should ask their processors prior to beginning an evaluation of their controls for privacy, information security and business continuity:

Question 1: Who - Which entities access, process or store/retain personal data?
Question 2: What - What types of personal data are accessed, processed, or retained/stored?
Question 3: Where - From what countries or locations does access, processing, and storage/retention occur?
Question 4: When - When did access, processing, or storage/retention start and end?
Question 5: Why - Is the purpose of usage authorized and defined in contract?
Question 6: How - How is data shared with other third or fourth parties?

Provider (processor) audits can leave an outsourcer (controller) with a good sense of the strengths or weakness of their security controls; however, without clarity on exactly what Target Data is being managed, where it is located, and whether the data is sent to other sub-processors. For example, the Client may not know about storage or transport services, disaster recovery/business continuity locations, or international contractors the processor may be using. Consequently, an audit may focus on the wrong data type(s) or location(s), or completely fail to evaluate environments where the data is stored. When the processor answers the six questions listed above, the controller is better able to examine the controls that are in place to protect data, wherever it may reside. The TDT also enables a trigger mechanism to capture if a particular location (e.g., datacenter or cloud providers) undergo independent audits or testing of controls.

Controllers may ask a processor to complete a TDT during pre-assessment or scoping in advance of a conducting a third party assessment using a Standardized Information Gathering (SIG) questionnaire or Standardized Control Assessments (SCA - formerly AUP) testing procedures. Alternatively, the processor may opt to complete a TDT prior to completing a third party assessment to ensure that the applicable data is in scope. A processor might also choose to complete the TDT in response to controller questions about how data is being managed or where it is located.

SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR Privacy Tool Kit – Target Data Tracker

Step-by-Step Instructions for Target Data Tracker

Initiated by processor:

1) Download the TDT from http://www.sharedassessments.org.
2) Decide whether you complete:
    a) One TDT for all controllers (identical services, data types, locations across clients); or
    b) Complete for a specific controller (due to diverse services, data types or locations).
3) Complete the information in the Target Data Tracker (TDT) sheet.
4) Send to the applicable controllers.

Initiated by client:

1) Processor will receive a TDT from their client.
2) Complete the information in the Target Data Tracker (TDT) sheet specifically for that Client.
3) Send to the Client.

Additional information - TDT scope:

Prior to undertaking to complete the TDT, the user should first define what is in scope for each of the following areas:

a) Target data types;
b) Company locations; and
c) Locations of processor sub-service organizations.

SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR Privacy Tool Kit – Target Data Tracker

Definitions

Client: An organization that outsources applications, systems or services to a Service Provider (Third Party).

Service Provider: An organization that provides outsourced services such as data processing, applications or systems to Clients.

Dependent Service Provider or Third Party: Organization(s) that provides outsourced services such as data processing, applications or systems directly to the Service Provider on behalf of the Client(s). May be called subcontractors, sub-processors or sub-service organizations, e.g., Service Provider contracted storage or transport services, Cloud Service providers, Disaster Recovery (DR)/Business Continuity Plan (BCP) location, contractors etc.

Target Data: Client's Non-Public Information (NPI), Protected Health Information (PHI), Personally Identifiable Information (PII), Personally Identifiable financial information, E.U. covered Personal Data, EU Special Categories of Personal Data and/or Consumer Report Information, that is stored, transmitted or processed by the Service Provider or Dependent Service Provider(s). Target data can also include any data selected as being in scope by the Service Provider or Client at the scoping of the engagement.

Additional Definitions are shown in the Glossary section of the SCA Privacy Testing Procedures included in the Appendices of this Tool Kit.

APPENDIX: TARGET DATA TRACKER	
QUESTION OR REQUEST	**RESPONSE**
Responder Name:	
Responder Job Title:	
Responder Phone Contact Information:	
Responder Email Information:	
Date of Response:	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
What is the Corporate office physical address?	
What is the Country of Origin or Incorporation of Company/Business?	
What is the location (entity & location) of any Backup site?	
Has the company completed any external assurance or security audits, if so provide date, and type/scope of assessment?	
Identify the type of external audit engagement?	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA DESCRIPTION	
What is the name and description(s) of all service(s) that are in scope for the TDT?	
What categories of data are accessed, processed, stored or retained?	**Enter Yes, No or Not Applicable for each category listed below.**
Consumer Report Information	
EU Covered Personal Data	
EU Special Categories of Personal Data	
Electronic or Personal Health Record	
Non Public Information	
Non Public Personal Information	
Personally Indentifiable Financial Information	
Personally Indentifiable Information	
Protected Health Information	
Higher Classifications of Protected Healthcare Information	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA DESCRIPTION CONTINUED	
Which entities access, process, or store or retain Target Data?	Enter Yes, No or Not Applicable for each category listed below.
Service Provider	
Employees	
Customers	
Third Parties, Subcontractors or Sub-Service Organizations	
Does the contract define and authorize data usage, data processing and/or data retention and storage?	
Is a retention period of Target Data defined and implemented?	
When did access, processing or storage/retention begin?	
Does the contract define disengagement requirements?	
Is a destruction period of Target Data defined and implemented?	
Identify the key safeguards in place for all service(s) that have been determined to be in scope for the TDT.	Enter Yes, No or Not Applicable for each category listed below.
Access to data is restricted by job role or function	
Target Data is sanitized or anonymized for access by third parties	
Target Data is encrypted for transmission	
Target Data is encrypted at rest or for storage or retention	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION	
Is this a shared service? (A shared service is provided to multiple clients, as opposed to a dedicated service provided to only 1 client.)	Enter Yes, No or Not Applicable for each category listed below.
Shared	
Dedicated	
Cloud Services	
Other, please describe:	
List the countries where Target Data is accessed	
List the countries where Target Data is processed	
List the countries where Target Data is stored or retained	
Please complete a location listing for each of your locations below:	
Please complete a location listing for each of your dependent service providers in scope below.	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Enter number of locations	
Location 1:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 2:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 3:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 4:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 5:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 6:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 7:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 8:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 9:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
VENDOR OR THIRD PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - YOUR LOCATIONS	
The purpose of this section is to document each of the locations where Target Data is accessed, processed or transmitted or stored and retained by you (the Service provider) for your Client(s).	
Location 10:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Specify if this is a Shared or Dedicated environment	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Enter number of Dependent Service Provider locations	
Location 1:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 2:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Company/business name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 3	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 4:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 5:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 6:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S') LOCATIONS	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 7:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 8:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 9:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

APPENDIX: TARGET DATA TRACKER	
SUB-PROCESSOR OR FOURTH PARTY INFORMATION	
What is the Sub-Processor's name?	
TARGET DATA LOCATION INFORMATION - SUB-PROCESSOR(S')	
The purpose of this section is to document each of the locations where Your Sub-Processor(s) access, process or transmit or store and retain your (the Service provider) Clients' Target Data.	
Location 10:	
Location Name:	
Physical Address (name, address, city, state, province, country, code)	
Description of product or service provided at this specific location	
Description of why the dependent service provider requires this data	
Provide the specific Target Data types that are provided (e.g., name, phone, credit information, SSN, medical, etc.)	
Is this a Shared or Dedicated environment?	
What is the Backup site location (name, address, city, state, province, country, code)?	
List any security audit(s) or assessment(s) that apply to this location and the date of completion of the audit(s) or assessment(s).	

SFG | SHARED ASSESSMENTS

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted source in third party risk assurance, is a member-driven, industry-standard body with tools and best practices, that injects speed, consistency, efficiency and cost savings into the control assessment process. Shared Assessments Program members work together to build and disseminate best practices, building resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments.

P: (505) 466-6434
F: (505) 466-3111
E: info@santa-fe-group.com