Date of Approval: 11/15/2024
Questionnaire Number: 1420

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Event Driven Architecture

Acronym:

EDA

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The EDA Project is establishing an Enterprise approach for the application of EDA including the stand-up of associated Platform components. The EDA Platform will serve as a distributed streaming platform, that will support the IRS developer community for building real-time data pipelines, streaming applications, and event-driven architectures.

The Confluent Kafka Technology Platform represents the core component of the EDA Infrastructure where it will act as the broker to enable event streaming within and across domains / applications. It provides the tools for storing, processing, and analyzing large datasets, as well as data integration and real-time processing. Furthermore, it offers a single platform for real-time and historical event data, enabling users to build an entirely new category of event-driven applications and create a universal event pipeline.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

Data including sensitive data shall come from various sources databases, applications, or other systems participating in an event driven workflow, where these producers shall send data to kafka brokers as topic data. Security measures such as SSL/TLS encryption shall be implemented to secure data in transit. Mutual TLS shall be used to authenticate all clients (producers/consumers), and brokers and Access Control Lists shall be used to control which producers and consumers can read from or write to specific topics. Data shall be stored with encryption at rest and data shall be replicated across multiple brokers for fault tolerance with proper encryption and security enabled. Topic management policies shall be implemented with proper and stricter access controls and encryption as well as ensuring retention only as long as necessary and compliant with IRS policy requirements. Consumers shall maintain secure access based on their access privileges. Retention policies shall be enforced to automatically delete data from Kafka topics after specific period that complies with the effective IRS policies. Compaction will be another feature that shall be used to remove old records and kept only to keep the latest version of data. Documentation and reports will be kept to maintain records of data destruction processes and audits as well as compliance reports of activities performed.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Centralized Authorization File (CAF)

Email Address

Employer Identification Number

Employment Information

Family Members

Federal Tax Information (FTI)

Individual Taxpayer Identification Number (ITIN)

Name

Preparer Taxpayer Identification Number (PTIN)

Social Security Number (including masked or last four digits)

Tax ID Number

Telephone Numbers

Vehicle Identification Number (VIN)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

Yes

1.2 What is the IRA Initiative Number?

Unknown

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

Enterprise Platform

1.35 Is there a data dictionary for this system?

No

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

Data including sensitive data shall come from various sources databases, applications, or other systems participating in an event driven workflow, where these producers shall send data to kafka brokers as topic data. Security measures such as SSL/TLS encryption shall be implemented to secure data in transit.

Mutual TLS shall be used to authenticate all clients (producers/consumers), and brokers and Access Control Lists shall be used to control which producers and consumers can read from or write to specific topics. Data shall be stored with encryption at rest and data shall be replicated across multiple brokers for fault tolerance with proper encryption and security enabled. Topic management policies shall be implemented with proper and stricter access controls and encryption as well as ensuring retention only as long as necessary and compliant with IRS policy requirements. Consumers shall maintain secure access based on their access privileges. Retention policies shall be enforced to automatically delete data from Kafka topics after specific period that complies with the effective IRS policies. Compaction will be another feature that shall be used to remove old records and kept only to keep the latest version of data. Documentation and reports will be kept to maintain records of data destruction processes and audits as well as compliance reports of activities performed.

1.4 Is this a new system?

Yes

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

No

1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

Not Applicable - New System

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Tech Insertion - Adoption

1.95 If this system has a parent system, what is the PCLIA Number of the parent system?

Not Applicable - No Parent System

2.1 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act? Contact Disclosure to determine if an accounting is required. Enter "Yes" or "No". If Exempt, type "Exempt".

Not Applicable - No outside disclosures

2.2 Please provide the full name of and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Enterprise Services Governance Board (ESGB)

3.1 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960?

No

3.3 Does this system use cloud computing?

Yes

3.31 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

TCloud, FR1801046750, 03/02/2020

3.32 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

3.32 Does the CSP allow auditing?

Yes

3.33 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

High

3.4 Is there a breach/incident plan on file?

No

3.5 Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?

Yes

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

Not Applicable - This system will act as a platform for tenants to publish and subscribe in an Event Driven Architecture style application, where the platform will retain the data in an encrypted form (analogous to middleware technology).

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

As a platform, no personal will maintain access to PII. Access will be granted ONLY to non-person service entities. Roles include the Producer and Consumer of the data. No platform personnel will maintain access. Data will be encrypted using a key exchange mechanism that involves both the producer(s) and consumer(s).

4.51 How many records in the system are attributable to IRS Employees? Enter “Under 50,000”, “50,000 to 100,000”, “More than 100,000” or “Not Applicable”.

Not Applicable

4.52 How many records in the system are attributable to contractors? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not Applicable”.

Not Applicable

4.53 How many records in the system are attributable to members of the public? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not applicable”.

More than 10,000

4.54 If records are attributable to a category not mentioned above in 4.51 through 4.53, please identify the category and the number of corresponding records to the nearest 10,000. If none, enter "Not Applicable".

Not Applicable

4.6 How is access to SBU/PII determined and by whom?

Determined by event Producers.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

None known at the time of form completion. Risk Analysis may identify risks which will be mitigated at a future date.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 Does this system use or plan to use SBU data in a non-production environment?

No

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

To maintain records of business tax returns, return transactions, and authorized taxpayer representatives.

Records Retention

What is the Record Schedule System?

Non-Record

What is the retention series title?

Data Destruction Upon Consumption

What is the GRS/RCS Item Number?

Not Applicable

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Not Applicable

What is the disposition schedule?

Not Applicable

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

BMF Retention Register

What is the GRS/RCS Item Number?

210

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

The records in the BMF DS to the BMF System are scheduled. Approved disposition instructions are published in IRS Document 12990, under Records Control Schedule 29 for Tax Administration-Wage and Investment Records, Item 210. In 1980, the National Archives and Records Administration (NARA) appraised the Information Returns as Temporary Records (Job No. NC1-58-82-9), but with a long-term storage requirement of 75 years after year of processing. Annual Conversion updates the BMF.

An analysis is performed and based on factors such as the current status, the assessment expiration date and collection expiration data entity and tax modules are removed to the retention register. A copy of the removed Entity will be put on the Microfilm Replacement System (MRS) Deleted Entity File for future research purposes. IRS follows disk sanitization procedures for destruction of discarded media. IRM 2.7.4, Management of Magnetic Media (Purging of SBU Data and Destruction of Computer Media) provides those procedures used for sanitizing electronic media for reuse (e.g., overwriting) and for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse (e.g., degaussing).

What is the disposition schedule?

75 years after year of processing