

**Privacy Impact Assessment (PIA)
for
Legal**

**Enforcement Decisions and Orders Salesforce
(EDOS)**



Date Approved by Chief Privacy Officer (CPO)/Designee:
1/28/2019

Section 1.0: Introduction

In accordance with federal regulations and mandates¹, the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).² The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

The Federal Deposit Insurance Corporation (FDIC) supervises the following entities and has the statutory authority to take enforcement actions against them:

- FDIC-insured state chartered banks that are not members of the Federal Reserve System;
- FDIC-insured branches of foreign banks; and
- Institution-affiliated parties (IAPs), such as officers, directors, employees, controlling shareholders, agents and certain other categories of individuals associated with such institutions.

¹ [Section 208 of the E-Government Act of 2002](#) requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum [M-03-22](#) provides specific guidance on how Section 208 should be implemented within government agencies. The [Privacy Act of 1974](#) imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, [Section 522](#) of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

² For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

Generally, the FDIC pursues enforcement actions against the above entities for violations of laws, rules, or regulations, unsafe or unsound banking practices, breaches of fiduciary duty, and violations of final orders, conditions imposed in writing or written agreements. In addition, the FDIC has the statutory authority to terminate the deposit insurance of any insured depository institution for violation of a law, rule, regulation, condition imposed in writing, or written agreement, or for being in an unsafe or unsound condition or engaging in unsafe or unsound banking practices.

The Enforcement Decisions and Orders Salesforce (EDOS) system provides the FDIC Legal Division with an automated, streamlined process to track and publish formal enforcement actions against financial institutions/banks that are regulated by the FDIC or against their Institution Affiliated Parties (IAPs) (e.g., bank officers and employees). The determination to pursue and enforcement action against a bank or its officer/employee is made by FDIC's Division of Risk Management Supervision (RMS), and/or by FDIC's Division of Depositor and Consumer Protection (DCP), in conjunction with the Legal Division. The types of enforcement actions can include consent orders, removal and prohibition orders, prompt corrective actions, and cease and desist.

The EDOS system is built on Salesforce and is designed to electronically route Enforcement Decisions and Orders (EDO) records and documents between the authorized users within the Legal Division who are required to review and approve the enforcement records before they are made available to the public on a public-facing website which is also built on Salesforce. The automatic routing utilizes data (entered manually) and a PDF document attachment (also uploaded manually) by the authorized Legal Division users for review and approval prior to publishing to the public site. During this time, the data is considered sensitive and will be stored (but not yet available to the public) in Salesforce's Government Cloud platform, which is FedRAMP certified at the moderate impact level. The data storage happens on servers on US soil. The data does not leave the geographic boundaries of the USA.

Once the data is approved for release, the EDOS system automatically publishes the enforcement decisions and orders onto the EDOS public website for access by the public. Members of the public will make use of a search feature which accommodates searching based on multiple criteria to retrieve and display matching results. The results will also indicate whether the original orders have been modified or terminated. The published data will include a subset of fields available to the Legal Division authorized users and is considered non-sensitive.

All data, both sensitive and non-sensitive, is stored in the Salesforce system.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

EDOS contains publicly available versions of enforcement actions taken against the following types of entities and individuals, per FDIC's statutory authority:

- FDIC-insured state chartered banks that are not members of the Federal Reserve System
- FDIC-insured branches of foreign banks
- Officers, directors, employees, controlling shareholders, agents and certain other categories of individuals (institution-affiliated parties) associated with such institutions

These enforcement actions include the full name of the respondent or party named in the enforcement action and details about the enforcement decision or order pertaining to this individual or entity. In cases where the respondent is an individual (as opposed to an entity), this information constitutes PII.

In addition to the respondent's (party) name and enforcement order, the EDOS database stores the following data elements related to the enforcement action: category, type, docket number, action code, bank name and address, issued date, termination date, and the Nationwide Mortgage Licensing System & Registry (NMLS) ID³ of the respondent. The individual's name, combined with the enforcement action information, is not publicly available while undergoing review, approval, and tracking in the FDIC Legal Division, but is made available to the public once the information is approved for publishing onto the public website. Any unnecessary PII, such as the respondent's address, is redacted from the order prior to uploading it into EDOS and consequently is not included in the published version of the order.

Please note that the EDOS application does not collect any information on individuals utilizing the public website.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

The information is used to facilitate the review and approval/decision-making process of determining if an enforcement action will be made available to the public.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

- a) Explain the business purpose/need requiring the collection of SSNs:
b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

Yes List any additional legal authorities:

No

- c) Is the SSN is masked or otherwise truncated within the system?

Yes. Explain:

No. Is it possible to mask or otherwise truncate the SSN within the system?

Yes. Explain how it may be masked or truncated and why this has not been implemented:

No. Explain why it may not be masked or truncated:

³ The NMLS ID is a unique number permanently assigned by the Nationwide Mortgage Licensing System & Registry (NMLS) for each company, branch, and individual that maintains a single account on NMLS. The NMLS ID improves supervision and transparency in the residential mortgage markets by providing regulators, the industry and the public with a tool that tracks companies and individuals across state lines and over time.

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

Yes. Explain:

No. Is it possible to restrict access to specific groups of users within the system?

Yes. Explain how access may be restricted and why this has not been implemented:

No. Explain why access cannot be restricted:

3.4 Who/what are the sources of the information in the system? How are they derived?

The enforcement action data containing PII is obtained from authorized individuals in RMS, DCP, and the Legal Division and manually entered/uploaded into the EDOS application by authorized Legal users.

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

No federal agencies are providing data for use in the EDOS application.

3.6 What other third-party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

No third-party sources are providing data for use in the EDOS application.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

No Explain: Per the FDIC’s statutory authority, it may pursue enforcement actions for violations of laws, rules, or regulations, unsafe or unsound banking practices, breaches of fiduciary duty, and violations of final orders, conditions imposed in writing or written agreements; and as such individuals cannot opt-out by declining to provide personal information or by consenting only to a particular use.

Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

Authorized internal users in the following groups will have access to data in the EDOS application for the purposes described below. These authorized users may only view and edit enforcement data and documents depending on their restricted privileges:

- FDIC Legal Division staff (including Legal Specialists and Legal Reviewers from the Legal Enforcement Section – to process and approve EDO data (e.g., Enforcement Orders and Administrative Hearing data) for public release
- FDIC Office of Communications (OCOM) staff (including Public Affairs Specialists) – to create the Press Release and publish EDO documents to the public site

- EDOS System Administrator – to monitor and manage the system and user access
- FDIC Division of Information Technology (DIT) staff and contractors, as well as FDIC Salesforce Integrator support contractors, – to build and support the EDOS solution to meet FDIC specifications

4.2 How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access.

Access to data in EDOS adheres to current FDIC information security and privacy policies and practices. All uses must have the approval of their Manager/Supervisor and the Legal Division EDO Program Manager before access is granted to the system. Access to EDOS is facilitated and managed using the FDIC Access Request and Certification System (ARCS). Once an ARCS request has been approved, the Salesforce Platform team sets up users in the system to utilize single sign-on into the production environment.

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

- No
 Yes Explain.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

Not applicable.

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The EDO program manager is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual EDOS users are responsible and accountable for assuring the proper collection and user of the data. The Program Manager also has overall responsibility for the EDOS application and is accountable for establishing the criteria, procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected.

4.6 What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

Contractors employed by FDIC’s Division of Information Technology have been integral in the design and construction of the EDOS application and will provide technical and maintenance system support of the system, but will not have access to the production environment except for the purposes of migrating data from the old system.

Each contractor who has access to the EDOS application and/or source data is required to complete the FDIC’s Information Security and Privacy Awareness Training, which includes the Corporate Rules of Behavior. They are also required to sign the FDIC Contractor Confidentiality and Non-Disclosure Agreement.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

Data will be checked for completeness by visual inspection performed by authorized EDOS users. Then data will be manually entered into the EDOS application. The EDOS application will alert the user if certain required information is missing as per validation rules.

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

Access to the EDOS application is authorized via the ARCS request process. Once logged in, the user's access is restricted based on his/her defined role/profile. The profile of the user dictates what data they can view and what actions they can take in the system. Additionally, all users of the system are required to complete the FDIC's Information Security and Privacy Awareness Training, which includes the Corporate Rules of Behavior. In addition, Salesforce has out-of-the-box audit management capabilities.

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

EDOS users will have numerous retrieval options for the data prior to it being published to the public, but primarily will use the respondent (party) name, bank name, or order docket number.

Once the data has been approved and published to the EDO public site, the public users will be able to run a search for Decisions and Orders based on an individual's name.

6.2 What kind of reports can be produced on individuals? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?

EDOS will allow users to execute fourteen (14) reports. All of the reports may contain an individual's name (bank and title) when available and associated with an Enforcement Decision or Order. All reports will be accessible through the EDOS application only.

6.3 What are the retention periods of data in this system? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The retention periods of data/records maintained within EDOS application are covered by FDIC Records Retention Schedules. The Corporation also follows guidance on permanent and temporary records disposition issued by the National Archives and Records Administration (NARA).

6.4 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

The EDOS application operates under FDIC 30-64-002, Financial Institution Investigative and Enforcement Records.

6.5 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

No.

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

The EDOS application is not consolidating data, but instead is a system that automates and facilitates the tracking, processing, approval, and publishing of FDIC enforcement actions by authorized FDIC users.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

No. The EDOS application is built on Salesforce, which is already in use by DCP and the Office of the Ombudsman. All FDIC EDOS internal users will be using PIV to logon to their computer systems and then utilize SSO to access the EDOS application.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

The EDOS application is not used to monitor individuals. The access to the application is limited to authorized users who must comply with FDIC privacy and security policies.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

Any exposure of privacy-related data could adversely affect the reputation of the Corporation. EDOS maintains publicly available versions of enforcement decisions and orders which contain PII about individual respondents. Although this information is considered publicly available, the FDIC maintains safeguards to protect against the potential fraud or theft from either an FDIC employee or persons outside the Corporation.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

The completion of this PIA does not result in changes to the high-level business processes of reviewing and publishing the enforcement orders. However, the new EDOS application will be built on Salesforce to replace the EDO application that was developed in Java using a third-party product, as the workflow engine.