FEDERAL DEPOSIT
INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Docket SharePoint
(Docket-SP)

July 2016

FDIC Internal System

Table of Contents

System Overview

The Legal Division of the Federal Deposit Insurance Corporation ("FDIC" or "Corporation") receives and tracks all Corporation documents related to FDIC-initiated administrative enforcement actions and cases against depository institutions and institution-affiliated parties. The Executive Secretary Section (ESS) provides direct administrative and legal support to the FDIC Board of Directors. It provides the logistical support for Board meetings, records the minutes, and maintains the official records of the Board. In this capacity ESS serves as the custodian of enforcement actions and case records on behalf of the Corporation. Though the actual enforcement actions and its documents are maintained and tracked in hard copy form and stored locally and offsite, ESS creates a summary index record of the enforcement actions in the Docket database for electronic tracking. Currently, the legacy Docket database does not have the capability to import or link documents to the enforcement action index records created in the database. Therefore, each enforcement action index record created has its documents manually tracked outside of the Docket database. ESS manually captures a small subset of key attributes for each enforcement action index record to track and facilitate future search and discovery activities. The Docket database stores more than 25 years of legal pleadings indexes.

Docket-SP application will replace the current manual indexing system from legacy Docket database. Going forward, Docket-SP will utilize the Enterprise SharePoint solution to index and retrieve enforcement and personnel action records that occur by consent without direct action by the Board of Directors. Moving to the SharePoint platform will provide greater functionality to ESS to track not only enforcement action index records, but also link documents to each enforcement action in the new application. All roles are maintained through NT user group definitions and Active Directory. Application access is role based.

Personally Identifiable Information (PII) in Docket-SP

Docket-SP is a privacy-sensitive project utilizing the existing SharePoint Solution to electronically store and manage enforcement actions and case documents (exhibits, etc.) and may contain agency-sensitive (i.e., bank closing information) and sensitive PII. Docket-SP has the ability to collect, generate and retain the following personally identifiable information (PII):

- Full name
- Date of birth
- Social Security number
- Photographic identifiers (e.g., photograph image, x-rays, and video)
- Driver's license/state identification number
- Biometric identifiers (e.g., fingerprint and voiceprint)
- Employee identification number
- Mother's maiden name
- Vehicle identifiers (e.g., license plates)
- Home address
- Phone numbers (e.g., phone, fax, and cell) (non-work)

- Medical information (medical records numbers, medical notes, or X-rays)
- Financial information and/or numbers (e.g., checking account number/PINs/access or security codes/passwords)
- Certificates (e.g., birth, death, naturalization, marriage)
- Legal documents, records or notes (e.g., divorce decree, criminal records, or other)
- Investigation report or database
- Web URLs (personal)
- E-mail address (non-work)
- Education records
- Military status and/or records
- Employment status and/or records
- Foreign activities and/or interests
- Legal exhibits which could potentially contain PII

Purpose & Use of Information in Docket-SP

Docket-SP collects PII for the FDIC Legal Division ESS. The ESS is the custodian of records, on behalf of the Corporation, related to FDIC-initiated administrative enforcement actions and cases against depository institutions and institution-affiliated parties.

Sources of Information in Docket-SP

The information in Docket-SP is derived from the legacy Docket application. The data in the legacy Docket databases are indexes of each enforcement action. The data entry for these index records are solely collected through manual population of the data fields.

Notice & Consent

Individuals cannot “opt out” by declining to provide personal information or by consenting only to a particular use. PII is collected for Docket-SP using mandatory fields. The data is transcribed from court/case documents and entered directly into Docket-SP by authorized ESS staff in Legal. Individuals do not have the ability to opt out of providing PII.

Access to Data in Docket-SP

Users in the roles of enforcement administrator, report generation specialist, and/or expression of interest (EOI/intern) within Legal ESS will have access to Docket-SP to enter the information transcribed from court/case documents. Moving to the SharePoint platform will provide greater functionality to ESS staff not only to track enforcement action index records but also to link documents to each enforcement action in the new application.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy in Docket-SP

The data within Docket-SP is transcribed from court/case documents and entered directly into Docket-SP by authorized ESS staff in Legal. The accuracy of the data entries correspond to the accuracy of data contained on the document and the person entering the data in Docket-SP.

Data Security for Docket-SP

An IAMS request will be needed to obtain access to Docket-SP, and there are user roles defined that allow for varying access levels.

The Docket-SP application is built on the SharePoint platform. It will utilize granular permissions and make use of secure infrastructure capabilities to secure data.

All Docket-SP data will have appropriate access controls to ensure only authorized users have access to the data for operations such as read, write, and update. Access to the Docket-SP application will be provisioned through the IAMS workflow, and only those users who are members of appropriate Active Directory/SharePoint groups will be granted access.

All functions in the application, including search and reporting functionality, will be facilitated through permissions and only those users who have appropriate access will be able to perform those functions, for example, performing a search or running a report.

The Audit Management feature of SharePoint will be used, as deemed necessary, to monitor create, read, update, and delete operations made to Docket-SP data to identify any potential misuses. SharePoint data use is monitored with customized audit trails to verify that data is being sent only as intended.

The System Owner is responsible for assuring proper use of the data. Also, it is the responsibility of every user (i.e., system administrator) to ensure the proper use of corporate data in accordance with FDIC Directives and the Corporate Information Security Awareness and Privacy Awareness Orientation, which include Rules of Behavior that focus on protecting sensitive information and sensitive personally identifiable information.

Contractors are employed by the FDIC to provide development and maintenance support for Docket-SP. Each contractor who has access to Docket-SP and/or source data is required to sign an FDIC Contractor Confidentiality Agreement. Contractors do not have access to the Docket-SP production environment.

System of Records Notice (SORN)

Docket-SP operates under the FDIC Privacy Act SORN 30-64-0003, *Administrative and Personnel Action Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.