IBM FileNet Image Services

GDPR Deployment Guidelines

Contents

GDPR overview

From May 2018, the General Data Protection Regulation (GDPR) applies not only to organizations that are located in the European Union (EU), but also to organizations that are located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects residing in the EU, regardless of the organization's location. For more information about GDPR, see IBM Security.

What is GDPR?

GDPR stands for General Data Protection Regulation. GDPR has been adopted by the European Union and European Economic Area (“EU”) and will apply from May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for companies and organizations that handle personal data
- Significant financial penalties for non-compliance
- Compulsory data breach notification

Notice

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn how you can ensure that your FileNet Image Services system and applications are GDPR ready.

Configuration for GDPR readiness

When configuring FileNet Image Services, if possible avoid creating any user indexes that may include personal data. Set up security groups and assign users to specific groups so that users only access documents they need. The granularity of access groups is at a document level which is inclusive of user indexes and image pages and generally managed based on the document class. Individual annotations may have their own access rights, but by default, inherit the documents' access rights.

FileNet Image Services depends on additional software products, such as, databases and storage devices (from Dell EMC, IBM, NetApp, and Hitachi). Make sure to consult the GDPR-readiness information for those prerequisite products when you configure your environment for FileNet Image Services.

Ensure only authorized access to the environment

In addition to controlling overall access to FileNet Image Services, you must also configure authorization for different areas and functions in the product. This configuration ensures that users access only the data that is relevant to their role within the environment and no more.

For information about setting up access and authorization in a new installation, see the Security Administration section in the IBM FileNet Image Services System Administrator's Handbook.

Encrypt user and password when communicating with client

User ID and passwords are always encrypted when communicating with a client. No configuration is necessary.

Encrypt content

Content encryption is not supported by Image Services natively. But any third-party encryption at the storage layer can be used in conjunction with MSAR, cache, or MKF database if it is designed to be transparent to applications and communication channels to and from storage. If Single Document Storage (SDS) is used, turn on transparent encryption on Storage device when possible.

Determine retention settings for objects

Plan your retention strategy to ensure that objects are retained only as long as there is a business need or as long as required by applicable regulatory requirements.

Prevent logging and tracing of sensitive information

If you encounter a problem with FileNet Image Services, you might need to provide trace logs to IBM support. These logs can contain personal data though it is extremely unlikely. Before you send a log file to IBM support, edit the file to mask any personal data, if there is any.

Data lifecycle: Use of personal data in FileNet Image Services

For each intended user of your FileNet Image Services system, it is required to set up user accounts by creating user IDs, passwords, groups, and privilege sets to allow users access to FileNet Image Services. Image Services uses MKF (proprietary database) Security DB to store user IDs and passwords. No other personal data is collected, such as, phone numbers, SSN, or birthdate. After the user account is set up, FileNet Image Services uses that account to authenticate the user and groups to determine the operations allowed for that user account. The granularity of access groups is at a document level which is inclusive of user indexes and image pages and generally managed based on the document class. Individual annotations may have their own access rights but by default, inherit the document's access rights.

In the process of defining individual user IDs, the FileNet Image Services administrator organizes them by grouping them together with other user IDs that have similar access needs or similar job requirements.

GDPR recommendations align with the required method to configure access to FileNet Image Services, creating users within Image Services groups to allow access to only what is necessary. Image Services stores passwords and user IDs in MKF security DB and this information is stored encrypted at rest.

Note:

For the purposes of this explanation, personal data refers to data that is gathered and used by FileNet Image Services. It does not include any personal data that is part of content that users of FileNet Image Services might store in FileNet Image Services. Your organization is responsible for identifying and controlling personal data as per GDPR rules.

Data collection: Controlling the collection of personal data

It is your organization's responsibility to determine what user data to collect. Personal data may be stored in FileNet Image Services as a customized user index that has been configured (that is, Birthday, SSN, or phone number user index), an annotation with personal data may be created, or a document image that may include personal data. These are all controlled by your organization.

FileNet Image Services does not collect personal data by default. It is up to your organization to determine what kind of data to include when users add or create content in the system.

Data storage: Controlling storage of personal data

Your organization controls how personal data is stored in your FileNet Image Services system. Personal data may be stored in FileNet Image Services as a customized user index that has been configured (that is, Birthday, SSN, or phone number user index), an annotation with personal data may be created, or a document image that may include personal data. These are all controlled by your organization. The only personal data that FileNet Image Services requires is user ID and password.

When storing personal data, consider decisions around logging, high availability, and disaster recovery.

Long term data storage

Whenever a user stores any content in FileNet Image Services, the initial user meta-data, such as user index values, are stored with the content. This is done so that the documents may be imported to another system or the restore can be used to recover initial indexing. Personal data may also appear in document images which are stored in secondary storage (that is, MSAR) and in temporary cache. Annotations may also have personal data and are stored in MKF permanent DB. It is recommended that the storage device encryption be enabled for secondary storage, cache, and MKF permanent DB files when possible as long as the encryption is designed to be transparent to Image Services.

Image Services does not perform data encryption of Relational Database where the user indexes are stored. If personal data is stored in user indexes, it is recommended that database native encryption be used or transparent data encryption (TDE) so that user meta-data will be encrypted while at rest. Note that there is a performance penalty when native database encryption is used due to the encryption and decryption processes.

Short term or temporary data storage

Image Services has elogs and other debug logs that might be turned on. It is possible that personal data might be included in the log but highly unlikely that user meta-data or user ID are written to a log. Annotation information and image content are never logged in FileNet Image Services. Tracking of Image Services security activity, such as login successful, login failures, and security changes may also be captured in log files. The security activity log does include user IDs. This may be disabled by using the Xapex Security Administration UI (select System window, select Default Security Settings, and clear Log setting options).

Replication of personal data for HA or disaster recovery

For business continuity purposes, FileNet Image Services may optionally be configured for high availability to ensure access to content even if there is a failure in one component of the product. There are different ways FileNet Image Services can be configured for high availability or disaster recovery. Although it is outside the scope of this document to provide detail on the methodologies for configuring FileNet Image Services for high availability or disaster recovery, most methodologies rely on replication of database and content storage used by FileNet Image Services.

With high availability, personal data may be replicated to another system and special care may be needed. In general, Image Services uses an active and passive high availability strategy. When this strategy is employed, there is only one set of storage and databases are shared between an active and passive system. If a problem occurs in the active system, the passive system takes over with the same set of storage and databases. In that case, there are no additional copies of information where personal data may be stored. When Multiple System Committal is used, there are copies of information in multiple Image Services systems. Information such as user indexes and document images, where personal data may be stored, can be copied between different active systems.

Use of personal data in backups

The FileNet Image Services administrator is responsible for making backups of FileNet Image Services by using Enterprise Back and Restore (EBR) or any off-the-shelf commercial backup and restore products.

Whenever a FileNet Image Services backup is made, you may be making a copy of personal data that is stored in FileNet Image Services. Your organization defines the policies that govern how long backups should be kept, who has access to backups, the process for logging access to backups, restoration from backups, and deletion of backup copies.

For example, if you have daily backup or periodic daily backup practice with a 30-day backup policy, then backups are kept for 30 days. Storage is then reused or recycled for new backups after 30 days, or backups are deleted after 30 days. This period can also be used to define a 30-day personal data deletion policy in which data from FileNet Image Services as well as the backup is removed after 30 days.

Data access: Controlling access to personal data

Users have access to data and content in FileNet Image Services. FileNet Image Services security is controlled by access groups and the granularity is at a document level and individual annotation level. Each Image Services object (document or annotation) has group access rights associated with it (read, write, and execute). It is not possible to control the access of individual user indexes, and hence, personal data cannot have different access rights from the rest of the document. It is possible to do that with each annotation. For example, it would be possible to create a text annotation and include personal information and then change the access group to SysAdminG so only users in the SysAdminG group could read this annotation.

Data processing: Controlling processing of personal data

Users have access to data and content in FileNet Image Services. It is not possible to set restrictions for individual user indexes that contain personal data. If your system requires personal data in user indexes, try to allow only the SysAdmin or SysAdminG to have access to these documents.

Encrypting personal data in motion

User ID and password are encrypted when going over the network. Other content is not encrypted when going over the network. If there is personal data in user indexes, in annotations, or in image pages, this information will not be encrypted while going over the network. RDB Database SSL may be used so that encryption may be used when database server and database client communicate.

Encrypting personal data at rest

User ID and password are always encrypted when stored in the MKF security database. User indexes are not encrypted when at rest unless native database encryption is used. Personal data may be stored in annotations. Annotation data is stored in MKF permanent database and if the storage device has an encryption capability, it should be enabled. Personal data may also be stored in image pages of documents. If it is, enable encryption in the secondary storage device and cache storage device when possible.

Data deletion: Controlling deletion of personal data

FileNet Image Services security uses access groups at document-level granularity. It is not possible to set user indexes access rights independently from the rest of the document so individual user indexes with personal data cannot have additional restrictions or protection. It is possible that user indexes with personal data may be modified or set to NIL value by a user who is in the read and write permission groups. The whole document may be deleted with meta-data by a user who is in the read, write, and execute group for that document.

Data monitoring: Monitoring access to personal data

FileNet Image Services does not provide audit logging of user indexes or annotations where personal data may reside. There is no monitoring capability in FileNet Image Services that may be leveraged.

Data subject rights: Determining and deleting personal data

Using the Database Maintenance UI, you can look at the existing user indexes to determine if there is any personal data on your FileNet Image Services system. For example, “SSN”, “phone number”, or “birthdate” index names would likely be personal data fields.

Deleting personal data for a user index

If you realize that your system has personal data in one or more user index, you can remove that personal data from the Image Services system by creating a ISTK, ISRA, or IDM custom application.

Revision table

Date	Description
24 May 2018	Initial release of document

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
J74/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, FileNet, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Itanium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

U.S. Patents Disclosure

This product incorporates technology covered by one or more of the following patents: U.S. Patent Numbers: 6,094,505; 5,768,416; 5,625,465; 5,369,508; 5,258,855.