IBM Aspera Drive Considerations for GDPR Readiness

For PID(s): 5725-S57

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Aspera Drive that you can configure, and aspects of the product's use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems.

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.

Table of Contents

GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union ("EU") and applies 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 processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

Read more about GDPR

- (EU GDPR Information Portal)[https://www.eugdpr.org/]
- (ibm.com/GDPR website)[http://ibm.com/GDPR]

Product Configuration - considerations for GDPR Readiness

References

1. *IBM Aspera Drive Admin Guide*
2. *IBM Aspera Drive works with IBM Aspera Faspex, IBM Aspera Files, and IBM Aspera Shares servers. Some security features must be configured on the server side. For information, see the documentation for these server*

How to configure our offering such that it could be used in a GDPR environment?

- Follow the installation instructions in the *IBM Aspera Drive Admin Guide*.

Data Life Cycle

What is the end-to-end process through which personal data go when using our offering?

List the personal data pieces the product collects and processes:

- Account data
  - Username
  - Password
- IP address
- Configuration

    - Server address
    - Credentials to server and storage
    - User preferences for IBM Aspera Drive
- Log data
    - Log of activity, performance, and errors
- User content (unknown/unclassified data)
    - Uploaded files or folders
    - Downloaded files or folders
    - Package metadata. What is included as metadata is configurable on the server side. For information, see the documentation for these servers.

Account data life cycle:

- Account data
    - When collected: IBM Aspera Drive collects account data when users or admins create or update accounts.
    - How collected: The user or admin inputs the account data into the program.
    - Where resides: The login credentials are saved in the OS keychain, and are encrypted.
    - When removed: The user can remove their account. For information, see the *IBM Aspera Drive Admin Guide*. In addition, when users uninstall the application, they can choose to remove all related data. For information, see the *IBM Aspera Drive Admin Guide*.
- IP address
    - When collected: When the user uploads or download files, IBM Aspera Drive records the IP addresses, and saves them in activity logs.
    - How collected: The application detects the user's IP address.
    - Where resides: In activity logs.
    - When removed: The user can manually delete logs at the OS level. In addition, when users uninstall the application, they can choose to remove all related data. For information, see the *IBM Aspera Drive Admin Guide*.
- Configuration
    - When collected: When the user configures their preferences for IBM Aspera Drive, after they have created an account.
    - How collected: The user inputs data to the configuration, or imports from a pre-existing configuration file.
    - Where resides: Login credentials are saved in the OS keychain, and are encrypted; configurations are saved in the configuration database (a SQLite database, located at ~/.aspera/connect/var/asperaconnect.data).

    - When removed: When users uninstall the application, they can choose to remove all related data. For information, see the *IBM Aspera Drive Admin Guide*.
- Log data
    - When collected: When the application is running. Users can choose different logging levels. For information, see the *IBM Aspera Drive Admin Guide*.
    - How collected: The application captures and generates related information.
    - Where resides: Logs reside in ~/Library/Logs/Aspera_Drive. Note that this log location may change in forthcoming releases of the application.
    - When removed: The user can manually delete logs at the OS level. In addition, when users uninstall the application, they can choose to remove all related data. For information, see the *IBM Aspera Drive Admin Guide*.
- User content
    - When collected: When the user uploads or downloads a file, IBM Aspera Drive caches the file in a hidden location: ~/.aspera/localcache. The application captures the metadata about the file and communicates it to the transfer server.
    - How collected: The application captures this information.
    - Where resides: User content resides in the local file system, transfer server, or storage type that has been chosen or configured by the user or the admin.
    - When removed: User content is removed when the user removes it from the local OS and from server storage. In addition, when users uninstall the application, they can choose to remove all related data from the local OS. For information, see the *IBM Aspera Drive Admin Guide*.

Data Collection

Data Collected by this product

- Account data
    - Username
    - Password
- IP address
- Configuration
    - Server address
    - Credentials to server and storage
    - User preferences for IBM Aspera Drive
- Log of activity, performance, errors
- User content (unknown/unclassified data)

- Uploaded files or folders
- Downloaded files or folders
- Package metadata: what is included as metadata is configurable on the server side.

Data Storage

Options to control/configure the storage of personal data

- Storage of account data
  - Drive saves the username and password, encrypted in the OS keychain. Server addresses are saved in the configuration database, a SQLite database, located at ~/.aspera/connect/var/asperaconnect.data.
- Storage of IP addresses
  - IP addresses are captured in the logs, which are in ~/Library/Logs/Aspera_Drive. Note that this log location may change in forthcoming releases of the application.
- Storage of configuration
  - Configuration data is saved in the configuration database, a SQLite database, located at ~/.aspera/connect/var/asperaconnect.data.
- Storage of log data
  - Logs are in ~/Library/Logs/Aspera_Drive. Note that this log location may change in forthcoming releases of the application.
- User content
  - IBM Aspera Drive transfers user content. This content may be stored in the local file system as OS file, in the hidden cache folder ~/.aspera/localcache, on a transfer server, or in other storage types. The application relies on the customer to control and protect the storage location. For more information on configuring storage on the server side, see the documentation for the server type (IBM Aspera Faspex, IBM Aspera Files, or IBM Aspera Shares).

Data Access

Controlling access to personal data

- Authentication
  - The program accommodates the authentication systems of the underlying transfer server.
- Roles and access rights
  - Roles and access rights on the server side are configured on the server.
  - Access rights to the local file system, including the hidden cache and logs, are configured by the local OS.
- Separation of duties

- The server admin and the user are in control of implementing the appropriate separation of duties.

Data Processing

Protecting personal data

- Data protection in motion
  - For user content transfers (uploading or downloading files), communication is on the secure Aspera FASP protocol.
  - Other management-type communication between IBM Aspera Drive and the servers is on the secure protocol HTTPS.
  - For IBM Aspera Faspex, users can configure the option "Encrypt sent files" to encrypt user content in motion. For information, see the *IBM Aspera Drive Admin Guide*.
  - For IBM Aspera Files and IBM Aspera Shares, the server admin can configure the option to encrypt user content in motion. For information, see the documentation for IBM Aspera Files and for IBM Aspera Shares.
- Data protection at rest
  - Customers can opt to encrypt user content on the server storage encryption-at-rest (EAR). For information, see the documentation for the transfer server products. If user data is transferred with EAR, the recipient must supply a passphrase to decrypt it. For information, see the *IBM Aspera Drive Admin Guide*.
  - Customers need to take appropriate action to protect the configuration database, log files, and user content on the local OS.
- Encryption of account data
  - Drive saves credentials, encrypted in the OS keychain.
  - Other account data and configurations are in the configuration database, unencrypted. Customers need to take appropriate action to protect the configuration database, log files, and user content on the local OS.
- Encryption key protection
  - When the user chooses to encrypt user content for uploading and to decrypt user content for downloading, the user must enter a passphrase as the encryption or decryption key. The application does not store the encryption/decryption key.

Data Deletion

- Deleting account data
  - Users can delete accounts. Users can also uninstall the application and choose to remove related data when uninstalling.
- Deleting user content

- The application relies on the customer to control the deletion of user content on the local OS.
- The application relies on the server admin to grant users of IBM Aspera Drive the appropriate permissions to delete user content on the server side.

Data Monitoring

- Monitoring
  - Users and admins can see an Activity window that shows the status of transfers and the location of transferred user content.
- Logging
  - Users and admins can see log files that show transfer activity, errors, warnings, and speeds.
  - On Windows, log files are located in C:\Users\username\AppData\Local\Aspera\Aspera Drive\var\log. On macOS, log files are located in ~/Library/Logs/Aspera_drive. Note that this log location may change in forthcoming releases of the application.
  - Log retention: the application relies on the user to remove logs and enforce log retention.
- Log file access control
  - The application relies on the user to enforce log access at the OS level.

Responding to Data Subject Rights

- Right to Access
  - Users have access to their account data.
  - Users have access to their user content on the local OS.
  - The server admin is in control of granting users of IBM Aspera Drive the right to access user content on the server side.
- Right to Modify
  - Users can modify their account data.
  - Users can modify their user content on the local OS.
  - The server admin is in control of granting users of IBM Aspera Drive the right to modify user content on the server side.
- Right to Restrict Processing
  - All personal data is collected and needed for the purpose of providing a service. However, users can choose not to use the service; can uninstall the application; and can request that the server admin remove their personal data from the server.
- Right to Object
  - All personal data is collected and needed for the purpose of providing a service. However, users can choose not to use the service; can uninstall

the application; and can request that the server admin remove their personal data from the server.

- Right to Be Forgotten
  - All personal data is collected and needed for the purpose of providing a service. However, users can choose not to use the service; can uninstall the application; and can request that the server admin remove their personal data from the server.
- Right to Data Portability
  - Log files can be easily read, moved, and processed.
  - The program does not provide a ready means for reading, moving, or processing account data or user content. It is the responsibility of the customer admin to provide a means for portability of account data.

Appendix

1. *IBM Aspera Drive Admin Guide*
2. *IBM Aspera Drive works with IBM Aspera Faspex, IBM Aspera Files, and IBM Aspera Shares servers. Some security features must be configured on the server side. For information, see the documentation for these servers.*
3. *Aspera Ecosystem Security Best Practices*