# IBM Aspera Client 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 Client 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 Desktop Client Admin Guide.

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

Follow the instructions in the Desktop Client Admin Guide to install the application.

---

## Data Life Cycle

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

The Desktop Client connects to High-Speed Transfer Server and High-Speed Endpoint through SSH connections.

### Data Types

- Account data
    - Remote operating system username
    - Remote operating system password or SSH public key
    - Object storage credentials (if connecting to object storage)
    - IBM Aspera Transfer Service (ATS) access key ID and secret (if connecting to ATS)
    - Roles and privileges

- IP addresses or hostnames
    - Client IP address
    - Server IP address or hostname
- Client and server configuration
- Logs
- User content
    - Uploaded, downloaded, and moved files

### Account Data Life Cycle

- When the user creates an SSH private-public key pair, the user is in control of the key files on the computer.

- When the user creates a connection in the GUI to a remote Server or Endpoint, they enter their SSH credentials, which are the system username and either the password or the path to the user's private key on the local computer. The user enters object storage credentials if the connection is to a remote Server or Endpoint in object storage. The account data are stored in configuration files and operating system keychain until the connection is deleted from the application by the user.

- When the user creates a connection to an ATS storage in the GUI, they enter their ATS access key ID and secret. The account data are stored in configuration files and operating system keychain until the connection is deleted from the application by the user.

- When the user starts an ascp, ascp4, or async session in the command line, they enter authentication credentials, as required. The SSH username and the path to the user's private SSH key are logged.

    - SSH credentials – The username is required. If using password authentication, the password is optional and can be entered at the prompt or set as an environment variable if it is not supplied in the command. If using SSH key authentication, the path to the private key on the local computer.

    - Object storage credentials – The user might include the access key ID and secret for the object storage, if the credentials are not added by the admin to the user's docroot.

    - ATS credentials – The user provides the ATS access key ID and secret as a basic token.

### IP Address Life Cycle

- Client and Server or Endpoint IP addresses are entered by users when they create a connection in the GUI or start an ascp, ascp4, or async transfer. IP addresses or hostnames are saved to activity logs. The information persists in the logs until the logs are overwritten or the admin removes the logs.

### Client Configuration

- When a user submits a transfer request through the GUI or command line, the client transfer configuration and server transfer configuration are compared and applied following precedence rules. The log records the final transfer configuration, which can include settings from the client and the server.

### Logs

- Desktop Client logs all activities. Transfer session details, including SSH username, path to the user's private SSH key and the remote host IP address or hostname, are logged. Passwords are not logged. Users can specify where the local logs are saved. Logs persist until they are overwritten or deleted.

### User Content

- When a user transfers content between Desktop Client and a High-Speed Transfer Server and High-Speed Transfer Endpoint, the content is encrypted during transfer by default. The user can configure the cipher to use for in-transit encryption. In-transit encryption only applies to content while it is transit. Encryption of the content on the client computer is controlled by the server admin and Desktop Client user, respectively.

- When a user uploads content to a High-Speed Transfer Server or High-Speed Transfer Endpoint, the source content is stored in the source directory on the user's computer. When a user downloads content from a Server or Endpoint, the content is stored in the destination directory on the user's computer. The user controls the content in their possession.

---

## Data Collection

### Data Collected by this product

- Account data
  - Remote operating system username
  - Remote operating system password or SSH public key
  - Object storage credentials (if connecting to object storage)
  - IBM Aspera Transfer Service (ATS) access key ID and secret (if connecting to ATS)
  - Roles and privileges
- IP addresses or hostnames
  - Client IP address
  - Server IP address or hostname
- Client and server configuration
- Logs

- User content
    - Uploaded, downloaded, and moved files

---

## Data Storage

### Options to control/configure the storage of personal data

#### *Storage of Account Data / IP Addresses / Server Configuration*

- Desktop Client stores SSH account data for connections to High-Speed Transfer Server and High-Speed Transfer Endpoint in user specific configuration files. Desktop Client relies on the user to control and protect system account data.
- Desktop Client stores IP addresses and hostnames in the logs. Desktop Client relies on the user to control and protect log data.

#### *Storage of User Content (Unknown/Unclassified)*

- Users control content on the computer.
- Users can encrypt their content before uploading it to an Aspera server or while it is stored on their local computer; for instructions see “Client-Side Encryption at Rest (EAR)” in the Admin Guide.

#### *Storage of Databases*

[Not applicable to Desktop Client]

#### *Storage of Backups*

The Desktop Client user has full control of the file system and to backup the application and data.

#### *Storage of Logs*

Desktop Client saves user activities in unencrypted logs. By default, the logs are overwritten on a rotation. Desktop Client relies on the user to encrypt, save, or archive logs and set retention policies.

#### *Storage of Archives*

Users can archive content in an archive directory on their local computer after it is uploaded to a server. The user has full control of the file system.

---

## Data Access

### Controlling access to personal data

#### *Authentication*

- Users restrict access to the computer by operating system authentication.

#### *Desktop Client Configuration*

- Users configure the firewall to prevent unauthorized access. For instructions, see "Configuring the Firewall" in the Admin Guide.
- Users keep system software and Aspera software up to date.

---

## Data Processing

### Protecting personal data

#### *Data Protection in Transit*

- By default, data is encrypted using AES-128 in transit between Desktop Client and Aspera servers.
    - Users can request a stronger encryption cipher than is set on the server in the transfer request; for instructions, see "Transfer Files in the GUI," "Ascp Command Reference," and "Ascp4 Command Reference" in the Admin Guide.
- Users can check the server's SSH fingerprint and prevent transfers if the fingerprints do not match. For instructions see "Ascp Command Reference in the Admin Guide.

#### *Data Protection at Rest*

- Users can encrypt their content before uploading it to the server or while it is stored on their local computer; for instructions see "Client-Side Encryption at Rest (EAR)" in the Admin Guide.

---

## Data Deletion

#### *Deleting User Content*

- Users can delete content on the remote server to which they have access.
- Users can delete content on their local computer.

---

## Data Monitoring

### *Monitor and logging*

- Users can view the activity logs for the entire application.
- Users can view content transfer progress in the GUI.
- Diagnostics data is saved in logs. Users can change the logging level to gather more data (though at the cost of performance).

### *Log Files*

- For the default log location, see “Log Files” in the Admin Guide.
- Users can configure different logging locations if allowed by the server configuration.
- The system admin has full file access control to the logs and can configure log size, location, and intensity. For information, see “Server Logging Configuration for Ascp and Ascp4” in the Admin Guide.

---

## Responding to Data Subject Rights

### *Right to Access*

- Users can access their account data.
- Users can access all personal data except for passwords.
- Desktop Client does not have the off-the-shelf functionality to single out a specific user’s data from logs or database backup.

### *Right to Modify*

- Users can modify their own account data.
- The activity log data cannot be modified by Desktop Client.

### *Right to Restrict Processing*

- Desktop Client requires all data to provide adequate service. The user is in control of restricting data usage for other purposes.

### *Right to Object*

- User is in control.

### *Right to Be Forgotten*

- Customer admin can remove any user from the active system. Desktop Client does not provide off-the-shelf functionality to remove data from logs. It is up to the customer admin to design a way to remove data from logs.

### *Right to Data Portability*

- Desktop Client does not provide off-the-shelf functionality to port individual user data from logs. Client admin needs to design a way to port user data.

---

## Appendix

1. IBM Aspera Desktop Client Admin Guide.