IBM Shares version 2 Considerations for GDPR Readiness

For PID(s): 5725-S60

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Aspera Shares version 2 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 Shares 2.x Admin Guide
2. Aspera Ecosystem Security Best Practice (found in Appendix of Admin Guide)

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

1. Follow the instructions in the *Aspera Shares Admin Guide* to install the application.
2. In the *Aspera Security Best Practices Guide* located in the Appendix of the *IBM Aspera Shares Admin Guide*, follow the instructions in the topics below:
   - Securing the Aspera Application
   - Shares 2.0
   - Securing Content in your Workflow
3. In the *Aspera Shares Admin Guide*, follow the instructions in the topics below:
   - Configuring Shares Security
   - Installing a Signed SSL Certificate Provided by Authorities

---

Data Life Cycle

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

Data Types:

- Account Data

  - Username
  - Password
  - First Name
  - Email
  - Roles & Privileges
- IP Address
- Server Configuration
- Logs
- User Content (Unknown / Unclassified)
  - Transferred Files
  - Uploaded Files
  - Downloaded Files

Account Data

- When admin creates a local user account, account data is saved in the database, until an admin removes the user.
- When admin imports a directory service user, Shares creates a new account for the user account data. Account data saved in the database, until an admin removes the Shares user.
- When admin imports a SAML user, Shares creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Shares. Account data remains until an admin removes the new Shares account.
- When users log in through SAML, Shares creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Shares. Account data remains until an admin removes the new Shares account.
- When an admin or manager adds a user to a group, organization, or project, Shares saves the membership and any configured permissions in the database, until an admin removes the user from the group, organization, or project or removes the user account.
- When an admin or manager promotes a user to an organization admin or project admin role, Shares saves the role and any configured permissions in the database, until an admin demotes the user or removes the user account.
- When an admin modifies permission to a share for a user or group, Shares saves the new permissions in the database, until an admin removes the user or group.

IP Address

- IP addresses are saved to activity logs whenever a user logs in. The information persists until the customer admin removes the logs.

Server Configuration

- When an admin adds a transfer node to Shares, Shares stores the node information in the database, until an admin removes the node.
- When an admin creates a share from the transfer node, Shares stores the share information and permissions in the database, until an admin removes the share.

- When an admin changes system configuration settings, Shares stores the settings in the database.

Logs

- Shares logs all activities. The logs persist until deleted according to the customer admin's retention policies.

User Content

- When a user uploads content to a share, the content is stored in the share's source node, until a user removes the content through the Shares UI, or the customer admin directly removes the content from the directory.
- When an end user downloads content from a share, the content is stored on the end user's workstation. At that point, it is up to the end user to handle the content.

Data Collection

Data Collected by this product

- Account Data
  - Username
  - Password
  - First Name
  - Email
  - Roles & Privileges
- IP Address
- Server Configuration
- Logs
- User Content (Unknown / Unclassified)
  - Transferred Files
  - Uploaded Files
  - Downloaded Files

Data Storage

Options to control/configure the storage of personal data

Storage in Account Data / IP Addresses / Server Configuration

- Shares stores account data on the Shares MySQL database. Only user passwords are encrypted on the database. Shares relies on the customer admin to control and protect the MySQL database.
- Shares stores IP addresses in the logs. Shares relies on the customer admin to control and protect the logs.

- Shares stores server configuration data on the Shares MySQL database. Shares relies on the customer admin to control and protect the MySQL database.

Storage in User Content (Unknown/Unclassified)

- Shares stores user content on configured Aspera nodes. Shares relies on customer admins of those nodes for encryption and local file permissions. Customer admins can take additional measures to control and protect their nodes by referring to the guidance provided by the *Aspera Ecosystem Security Best Practices* document as well as the GDPR guidelines for *IBM Aspera Enterprise Server*.
- Admins can manage content storage location through Shares and can configure user permissions and access to the content. Shares relies on the customer admin to manage permissions in Shares.
- Shares relies on the end user to control and protect user content downloaded from Shares.

Storage in Databases

- The MySQL database can be on the same server as the application or on a separate database. Shares relies on the customer admin to control and protect the database and its host server.

Storage in Backups

- Admins can backup the MySQL database and configuration files with a backup script in an unencrypted backup directory. Shares relies on the customer admin for encryption, storage location, and retention policy.

Storage in Logs

- Shares saves user activities in unencrypted logs. User activities include: user login, change of management, and access to client data. By default, the logs will be overwritten in a rotated manner. Shares relies on the customer admin to encrypt, save, or archive logs and set retention policies.

Storage in Backups

- Customer admin has full control of the backup files.

Storage in Archives

- Shares does not have archiving features. Customer admin has full control of archive files.

Data Access

Controlling access to personal data

Roles and Access Rights

Customer admin can create user accounts with the following roles:

- System Admin: System admins can configure all system, user, group, and shares settings and permissions. They can also elevate users to managers or admins.
- Organization Admins: Organization admins can create and manage projects and make available users managers of projects, but they cannot configure permissions for admin users or configure permission for organizations they do not manage. Organization admins can also create and manage shares and configure share permissions for individual users. If given extra permissions, organization admins can add users outside of their organization to their organization.
- Project Admins: Project admins can create and manage shares and configure share permissions for individual users.
- User: Users can only access data they are given permission to access.

See *Understanding User Roles and Share Authorization*.

Separation of Duties

See Roles and Access Rights section above.

Authentication

Shares supports two methods of authentication: username / password and SAML.

Authenticating with Username / Password

- The username and password is provided by the user during initial registration or configured by an admin. Shares saves both into the database, but encrypts only the password.
- Admins can configure Shares to import Directory Service users and groups. Those usernames and passwords are handled as above.

Authenticating with SAML

- Shares saves usernames but does not save passwords. The SAML IdP is responsible for security of user passwords.

Data Processing

Protecting personal data

Data protection in Motion

- Admins can configure Shares to initiate transfers using AES-128 encryption mode. See *Configuring Transfer Settings*.

Data protection at Rest

- Admins can configure encryption-at-rest (EAR) on Aspera Nodes to store content uploaded to the server in an encrypted state. When downloaded from the server, server-side EAR first decrypts the files and then transfers the files to the client's disk

in an unencrypted state. For more information, See the *Aspera Enterprise Server Admin Guide: Server-Side Encryption at Rest (EAR)*.
- The encryption key for EAR is saved in the aspera.conf configuration file as cleartext. The customer admin needs to take proper protection to avoid unauthorized access.
- Shares relies on the customer admin to handle account data, content storage, and access to databases and files on the server.

Data Deletion

Deleting User Content

- Customer admin can delete content on a share.
- Customer admin can give other users permissions to delete content on a share.

Deleting Account Data

- Only admin accounts can remove user accounts.

Data Monitoring

Monitor and logging

- Managers and admins can access the admin activity log of shares they manage to see every permission and content change on the share.
- Admins can see an activity log for the entire application.
- Diagnostics data is saved in logs. Admins can change the logging level to gather more data (though at the cost of performance).

Log Files

Shares logs can be found in the following locations in the installation directory:

- www
- statscollector

Customer admin has full file access control to the logs.

Responding to Data Subject Rights

Right to Access

- End users can access their account data.
- Customer admins can grant or revoke a user's permission to access certain customer data.
- Customer admins can access all personal data except for passwords.
- Shares does not have the off-the-shelf functionality to single out a specific user's data from logs or database backup.

Right to Modify

- End users can modify their own account data.
- Customer admins can modify any user's management data.
- Customer admins can grant or revoke a user's permission to modify certain customer data.
- The activity log data cannot be modified by Shares.

Right to Restrict Processing

- Shares requires all data to provide adequate service. Customer admin is in control of restricting data usage for other purposes.

Right to Object

- Customer admin is in control.

Right to Be Forgotten

- Customer admin can remove any end user from the active system.
- Shares does not provide off-the-shelf functionality to remove data from logs or database backups. It is up to the customer admin to design a way to remove data from logs and database backups.

Right to Data Portability

- Shares does not provide off-the-shelf functionality to port data from logs or database backups. It is up to the customer admin to design a way to port user data.

Appendix

1. IBM Aspera Shares 2.x Admin Guide
2. Aspera Ecosystem Security Best Practice (found in Appendix of Admin Guide)