Tables of Contents

IBM Planning Analytics Local considerations for GDPR readiness

For PID(s): 5737-B03

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Planning Analytics Local 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.

IBM Planning Analytics Local 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 Overview

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 companies and organisations handling personal data
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

This document is intended to help you in your preparations for GDPR readiness.

Read more about GDPR

- EU GDPR Information Portal
- ibm.com/GDPR website

Product Configuration - considerations for GDPR Readiness

The following sections provide considerations for configuring Planning Analytics Local to help your organization with GDPR readiness.

Configuration to support data handling requirements

The GDPR legislation requires that personal data is strictly controlled and that the integrity of the data is maintained. This requires the data to be secured against loss through system failure and also through unauthorized access or via theft of computer equipment or storage media.

Data Life Cycle

IBM Planning Analytics stores data in different locations as it is populated into the system. The data that is stored depends on the effort that an administrator or modeller puts in. Data can be stored in the following locations:

IBM TM1 Server

}Clients dimension - can contain the UID as defined in the LDAP or an alias based on the CAMID in IBM Cognos Analytics.
}ElementAttributes_}clients - can contain a caption value as entered by a modeler. To delete this value, remove the caption or delete the element name in the }clients dimension.
}PerfClients - can contain the names from the }clients dimension entries which can be user name-specific. This can be considered personal data. To delete this, delete the element name from the dimension.
Transaction log - the tm1s.log records cube value changes.
Audit log - records changes to data or metadata.

Planning Analytics Workspace

Planning Analytics Workspace books can contain user identified information its naming convention. For example, Therese's book. Planning Analytics Workspace users can use names that contain personal information for anything they want. When the Planning Analytics Administrator capability becomes available, an administrator will be able to add email addresses which are considered personal information. Email addresses are entered in the Alerts tab. They can be the same across all TM1 databases or specific to individual addresses.

IBM Cognos TM1 Architect

Cognos TM1 Architect does not programmatically capture personal data about a user. Content that is created and committed through Cognos TM1 Architect is captured and stored at the IBM TM1 Server level.

IBM Cognos TM1 Perspectives

Cognos TM1 Perspectives does not programmatically capture personal data about a user. Content that is created and committed through Cognos TM1 Perspectives is captured and stored at the TM1 Server level. A model developer can populate metadata in the Excel sheet that references personal data. For example, a hidden sheet that drives a value in another place in the form. This metadata is a Microsoft Excel cell which can contain detail entered by the sheet editor.

IBM Cognos TM1 Application Web

Cognos TM1 Applications do not programmatically contain personal data about a user. If a user has access to a node in a Cognos TM1 Application Web application, deleting the user from the node access level removes any reference points.

Cognos TM1 Applications allow document attachment and node level commentary. Both items can contain personal information because they support free form text entry.

IBM Cognos TM1 Performance Modeler

Cognos TM1 Performance Modeler does not programmatically capture personal data about a user. Content that is created and committed through Cognos TM1 Performance Modeller is captured and stored at the TM1 Server level.

Data Collection

TM1 Server

TM1 Server cube data contains text based data so it can retain user detail. For example, a headcount forecast model with a dimension that has an element of Name. User details are not captured automatically, but as a database it can contain personal information that is entered by an administrator. Detail can also be written to alias values and they can be dimension element names. Anything that can be named or typed into a cell can have personal information about an individual. Another example is a salary planning cube has user name, user Id, employee number, salary, location, band, and so on. Any dimension or cube can contain this information.

Information created by an administrator or modeler for a TM1 Server model is stored in the data directory in a set of proprietary files. For more information about the data directory, see Data directory overview in the TM1 Installation and Configuration Guide.

Planning Analytics Workspace

Planning Analytics Workspace stores data about its users in BSS, its provisioning database. The information it stores includes User ID, full name, role, activation status, and user email.

Data is also stored in MongoDB. The information stored in MongoDB includes a user's assets and his permissions to those assets (view, view and edit, or full control). The assets, views, websheets, and books

collectively represent metadata that reference TM1 objects. Apache CouchDB contains the user's chat history and photo. The user's server tree bookmarks, history, and preferences are stored in Redis. Logs are stored in the logs directory and are organized by folder for each microservice.

Planning Analytics Workspace logs are debug mode logs. Planning Analytics Workspace microservices use the same AspectJ log injection service and they log all activity through the system.

This persistence architecture applies to all microdevices that support book authoring, contribution, modeling, life cycle management, administration, and on demand services.

Data Storage

IBM Cognos TM1 data is stored within a set of proprietary files. These files are located within either the data or data and logs directory as defined by the administrator. Both the data and logs directory are defined in the tm1s.cfg file. Access to these locations should be secured by using the Operating Systems file system access security mechanisms using properly defined access controls.

Data stored in TM1 Server (release 2.0.4) can have encryption at rest enabled, which will encrypt all content in the data directory and logs at rest. An administrator must configure encryption at rest. For more information, see TM1 server data encryption.

Planning Analytics Workspace encrypts all data at rest, except for the logs directory. A number of databases are included in the Planning Analytics Workspace install. They are, Redis, MongoDB and the BSS database referenced earlier. The Redis, MongoDB, and BSS databases are all encrypted by default.

Data Access

TM1 Server

Users can access data with proper authorization and authentication to objects as defined by the security administrator. Data can be secured at a model, cube, dimension, element, or cell level, which provides a robust set of capabilities to secure content. Data is accessed through Microsoft Windows based clients such as Cognos TM1 Perspectives or web-based clients. TM1 Server data is available through a proprietary C API or a RESTful API.

Planning Analytics Workspace Local data with proper authorization and authentication to objects as defined by the security administrator. A user can be authorized to access Planning Analytics Workspace Local without having access to any of the underlying TM1 Databases.

Data Processing

Planning Analytics is SSL-enabled for all communication. TM1 Server provides pre-configured signed certificates with 2048 bit AES 256 level encryption. All clients (provided or custom built) must use the secured certificate to authenticate and display TM1 Server data. You can also use custom certificates.

Data Deletion

TM1 Server

From the current application (.dim /.cub/etc) You can remove personal data by manually removing the element or cube intersections that contain the personal data. For example, in a salary forecast cube, the row within the cube, including potentially the element name, must be deleted. To do the deletion, you can write a TurboIntegrator script that reads metadata and data looking for specific name references and deleting or overwriting them.

}ElementAttributes_}clients - This control cube can contain a caption value. To delete this value, you must remove the caption or delete the element name in the }clients dimension.

}PerfClients - This control dimension can contain the names from the }clients dimension entries, which could be user name-specific. Delete the element name from the dimension.

From archives

You can remove personal data from archives by restoring the archive and manually removing the data in the same way you do it for the current application.

From logs

You can remove personal information from logs by destroying the log files or opening the files and searching and deleting the entries.

Planning Analytics Workspace

Deleting a user from Planning Analytics Workspace deletes the user, their assets, and all personal content. This functionality is available as of release 32.

Cognos TM1 Application Web

Cognos TM1 Application Web content can contain both attached documents and text-driven commentary. Your application administrator must open the individual applications to determine if the attached or custom commentary text contains personal information. This is a manual process that you must do for each application.

Data Monitoring

You can monitor user activity in Planning Analytics using tools such as Planning Analytics Administration, TM1 Top, and IBM TM1 Operations Console. These tools do not monitor the data flow. Data monitoring capabilities are done through the audit or transaction logs listed previously. For data monitoring, refer to the guidance provided there.

Responding to Data Subject Rights

IBM Planning Analytics stores data at rest both in log files and within the model structure of IBM Cognos TM1 Databases and Planning Analytics Workspace databases. The administrator must be aware of and remove any personal data based on Data Subject requests.