Tables of Contents

IBM Cognos PowerPlay considerations for GDPR readiness

For PID(s): 5724-W68

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Cognos PowerPlay 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 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 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 GDPR website: http://ibm.com/GDPR

Product Configuration - considerations for GDPR Readiness

The following sections provide considerations for configuring IBM Cognos PowerPlay to help your organization with GDPR requirements.

You use IBM Cognos Transformer to author a dimensional model based on data from one or more data sources. Then you create one or more multi-dimensional cubes based on the model and the data in the referenced data sources. An IBM Cognos Transformer model does not usually contain personal information because personal information is captured in the generated cubes in the form of category (member) short and long names, or category codes. You should update IBM Cognos Transformer models that make use of personal information as the identifier of calculated or manual categories to avoid the use of this type of data.

A cube produced from an IBM Cognos Transformer model can contain personal information if that is the level of detail to which information is captured. If data in a cube is not at that level of detail, then there are no data privacy issues unless the higher level of aggregated information is insufficient to disambiguate individuals (or a single individual). Your organization must make this determination for each cube in your system.

As with all cubes, but especially for those that contain personal data, ensuring a cube is password protected adds a level of security by encrypting the data in the cube. In addition, the application of user-based security to a cube can restrict users to accessing data for which they have is a legitimate business purpose.

For more information about Cognos Transformer security, see Adding security in the *IBM Cognos Transformer User Guide*.

If you have cubes for escrow or regulatory purposes, you should have appropriate encryption and access controls in place to control access to the data is limited to those with a legitimate business purpose.

The IBM Cognos PowerPlay Windows client or IBM Cognos PowerPlay Studio reports can contain references to categories (members). When a report is run after a category has been updated (for example, short name), the report reflects the change. If a category no longer exists, it is removed from the PowerPlay report and a warning is displayed that a category was not found. The category is not named in the message.

If a user retrieves and views the underlying report specification in text format, a category that identifies an individual can be viewed. If users can access files this way, then you should do a search and replace of the personally identifiable information associated with the GDPR user request.

Data Life Cycle

When you build an IBM Cognos Transformer model, you must know which columns in the model's data sources represent personally identifiable information. You must determine this information for all the data sources in IBM Cognos Transformer models in your organization.

If an IBM Cognos Transformer model includes dimensions made from one or more columns containing personally identifiable information, then cubes from the model of one of these dimensions must be rebuilt when you receive a GDPR-related request. For example, a request to update an individual's data or to be forgotten. You must update the cubes after the underlying data sources have been updated to reflect the individual's request.

If personal data is used to construct categories in dimensions of an IBM Cognos Transformer model (For example, a manual category with a short name that includes an individual's name), then you must update the model, independent of any updates to the underlying data sources.

Data is captured in source data systems such as data warehouses and Microsoft Excel spreadsheets. A dimensional model is created that defines a multi-dimensional structure based upon one or more of these sources of data. Cubes are then built from the source data based upon the defined dimensional data. Categories (members) and data values in a cube are based upon values in the data sources. The categories and data values in a cube can only be modified by rebuilding a cube.

IBM Cognos PowerPlay Windows client and IBM Cognos Transformer do not collect user personal data as part of their configurations. Therefore, it is not necessary to manage any GDPR-related requests for individuals who have the products.

IBM Cognos Transformer has two parts:

1. A user interface used to model dimensional cubes
2. An engine for the construction of cubes based upon one of these dimensional cube models

Personal data is contained in an IBM Cognos Transformer cube model in the following ways:

- The long or short name, or the code of a category (member) constructed from source data
- The long or short name of a manual category created in the model

The first form of category can be updated or removed from a cube by updating the underlying (original) data source (for example, a corporate data warehouse) and then rebuilding the cube.

The second form of category can be modified only by editing the cube model and then rebuilding the cube.

If a cube does not contain a dimension with categories representing any personal information, then the cube does not need to be updated for any GDPR-related requests unless the categories are related to individuals.

In a time partitioned cube, it is possible that an individual is contained in a subset of the partitions of the cube. In this example, we will assume a cube has been time partitioned.

If a person has requested to be forgotten, their data must be removed from, or anonymized in, all the partitions of the cube to so that none of their data is processed in the future. Then you must rebuild all the cubes to reflect the changes in the source data.

It's possible that existing historic cube partitions no longer have the original data that was used to build the cubes. This does not excuse the Controller from responding to a GDPR request. You must create a series of list reports that extract all the non-calculated values from the cube that generate a series of data files. Then you can edit the files to accommodate the current GDPR user request, update the corresponding model to use the newly created files, and rebuild the cube.

Data Storage

IBM Cognos Transformer can generate cubes which are password protected. You can also apply user-based security rules to control access to data in the cube. The combination of both security method can help restrict users to accessing data for which there is a legitimate business purpose.

Backups of cubes should be secured and access controlled and logged for audit purposes.

Data Deletion

As described previously, it is necessary for the people who have the responsibility for building cubes to do so after the underlying data sources have been modified to reflect a data subject's request. All affected/related reports must then be updated.

Data Monitoring

You should monitor the dimensions in IBM Cognos Transformer models that contain personal data. These cubes must be modified for GDPR-related requests.

You should regularly test, assess, and evaluate the effectiveness of your technical and organizational processes to comply with GDPR. These processes should include ongoing privacy assessments, threat modelling, centralized security logging, and monitoring, among others.

Responding to Data Subject Rights

As described previously, you must handle requests from a data subject by updating the underlying data sources, rebuilding the affected cubes, and then updating affected reports to remove or update references to the affected categories.

This is required for models, cubes, and reports that contain categories based on personal information.