IBM Incentive Compensation Mgmt-v10 considerations for GDPR readiness

IBM Confidential - till approved by IBM Legal.

For PID(s): 5725I02

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Incentive Compensation Management 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.

IBM Confidential - till approved for publishing.

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

The following sections provide considerations for configuring IBM Incentive Compensation Management to help your organization with GDPR readiness.

Configuration to support data handling requirements
Data residing in the system is largely safeguarded against loss or exposure due to system failure, however a regular database back-up process is strongly recommended. Unauthorized access is prevented via user authentication either native to the tool, or through Single Sign-on integration with customer's other systems. In the event that a user's computer is stolen, they are required to report the theft immediately so that their authentication credentials can be reset and/or their access can be temporarily suspended

Online content, user guides, and other manuals for Incentive Compensation Management: https://www.ibm.com/support/knowledgecenter/SSGKS6

Configuration to support Data Privacy
SPM supports data privacy by allowing for any individual's personal data to be visible only to the following persons:
 - themselves
 - their manager(s) and those further up in their management hierarchy
 - Compensation administrators responsible for validating and processing the individual's variable compensation

This is achieved via Web User Security Filter, restricting data sources against the Payee Hierarchy, and in some cases the use of Data Forms within the Admin Client.

Provided all instances of personal information have been identified and appropriate access restrictions have been put in place. It is possible in the tool to create a report without applying the appropriate access restrictions, so care must be taken to always include these.

Configuration to support Data Security
Within the system itself, Data Security is handled as above (see "Data Privacy". Additional data security measures are strongly recommended, including IP Whitelisting and typical IT security measures for the server on which the solution resides. Particular care should be given to the handling and processing of inbound and outbound data feeds.

Data Life Cycle

GDPR requires that personal data is:
* Processed lawfully, fairly and in a transparent manner in relation to individuals.
* Collected for specified, explicit and legitimate purposes.
* Adequate, relevant and limited to what is necessary.
* Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
* Kept in a form which permits identification of the data subject for no longer than necessary.

It should be noted that ICM itself is a tool, and is used to build systems according to the customer's own business process.
Typically personal employee data is received via an HR feed, with the customer being responsible for the secure generation, transfer, and import of this data into the ICM tool. The system then maps this against transactional sales data and calculates employee achievement against targets and resulting compensation values. These results – including some level of the employee's personal data –is then viewable in web-based reports, ie. through a web browser, accessible to the employee and their management chain, and can be exported to flat files for consumption by downstream payroll systems (again, with the customer being responsible for the secure handling of this data once it leaves the ICM tool).

Checks
As ICM is a tool to build the customers own model, there is no inbuilt data lifecycle which can be documented. As before, there is no predefined lifecycle to document

Determine the purpose for obtaining, processing and/or storing the data:
*** Contractual obligation**
*** Legitimate basis for processing**

Identifying Data (PI) about the employees is needed within the system to calculate their performance against target(s), so as to calculate and process their resulting variable compensation. This is to support the contractual obligation to compensate them as defined in the employee's Compensation Agreement.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

GDPR Explicit requirements:

1. Ensure the appropriate consent is in place - contract, service, explicit Data Subject consent
Customer has the ability to include an "acceptance of data terms and conditions" screen and workflow –or to include consent in a "Plan Acceptance" workflow. It is also possible to hold/maintain consent workflow outside of the tool, ie. within standard employment terms between the employer and employee.

2. Understand where the data resides in the application/solution
This is supported by the tool –ie. identifying tables / calculation result sets / reports / exports that contain employee personal data.

3. Ensure the data is secured through:
*encryption,
Various levels of encryption are available / supported
* access control,
Supported
* additional controls
IP Whitelisting is recommended

4. Ensure the retention period of this data is clearly defined
As the SPM system utilizes data (including personal data) to calculate and process financial activities, there are regulations requiring that historical data be stored for auditability purposes. The amount of historical data required can vary by industry and geography

5. Ensure the data is deleted at the end of the retention period
Due to the relational aspect of the data processing, outright deletion of data within the tool is not recommended, and can have a cascade effect on other critical historical data. There are two recommended approaches to addressing this requirement:
Anonymization of personal data. This is supported but typically requires some additional upfront configuration
Archiving of historical data in a flat format, so as to remove dependencies and allow for targeted data deletion

6. Ensure all the Data Subject rights can be fulfilled:
Higher standards for privacy policies and statements and for obtaining consent
Easier access to personal data by a data subject
Enhanced right to request the erasure of their personal data
Right to transfer personal data to another organization (portability)
Any personal data within the system can be easily exported to Excel / Acrobat / flat file formats.
Right to object to processing now explicitly includes profiling
Profiling is not a typical or recommended activity in ICM

Personal data used for online contact with IBM

Typically, only the client name and email address are used, to enable personal replies for the subject of the contact, and the use of personal data conforms to the [IBM Online Privacy Statement] (https://www.ibm.com/privacy/us/en/).

Data Collection

Typically this includes:
- Employee Name
- Employee ID
- Email address

…and may include:
- Employee mailing address
- Employee salary

Customer has the ability to include an “acceptance of data terms and conditions” screen and workflow –or to include consent in a “Plan Acceptance” workflow. It is also possible to hold/maintain consent workflow outside of the tool, ie. within standard employment terms between the employer and employee.

Standard write-back Presenter report and, if desired, an accompanying workflow.

Types of Data Collected

This does not apply, because ICM typically does not, itself, collect any data from end users, nor does it define what particular data should be collected – that is entirely a reflection of the customer's own terms of incentive compensation. The client imports data into the tool that they have already collected.

ICM does include a privacy notice on the main screen log in page.

Data Storage

IBM recommends that client's encrypt the IBM Incentive Compensation Management (ICM) database due to the personal data of producers stored in the system - see section Configuration to support Data Security above.

Protection is provided through user access control. End users are required to authenticate their identity (either through the application native method or with SSO) to access any data. The product provides the means to apply access control to any data it presents to the end users, although it is the customers own responsibility to specify what data is controlled and ensure the control is in place.
Privileged users (admins) who are able to access all data within the system are also required to authenticate their identity.
Each customer will have their own specific set of data, so there is no predefined documentation.

Ultimately, data is physically stored not within the product (ICM) itself, but in a database which is either on premise and subject to the customer's own access management control, or is on IBM Cloud.

Data Access

Data can be accessed by the end users, (typically) by their managers, and by administrators. The product provides mechanisms to define relevant roles and to control what data is presented to each, though customer themselves must define and put these in place.

Data Processing

Data is received (typically) from HR and Sales systems, and sent (typically) to finance and payroll systems. The customer themselves are responsible for the control of the data to and from the boundaries of ICM. Within ICM, all data is contained within a third party database (Microsoft SQL Server) which manages secure storage.

Once data (as defined by the customer) leaves their ICM system, it will go to their own downstream business process. Logical and physical access to the data is controlled by the customer themselves in the case of on-premise, or based on authenticated secure login (SFTP) when on-cloud.

Either according to the customer's own database management procedures if on -premise, or provided by IBM Cloud. If on premise, as defined by the customer themselves - Hosting, storage, backup

At the physical database level, either restricted to Cloud personnel, or on premise in accordance with the customer's database management policy.
At the application level, support, administration and maintenance are provided by privileged users (admins) in accordance with the customer's IT policy.

All data is securely held within a relational database
In on-premise deployments, the client is responsible for encryption, maintaining the key, and working with the data.

Data Deletion

Article 17 of the GDPR states that data subjects have the right to have their personal data removed from the systems of controllers and processors - without undue delay - under a set of circumstances.

The user guide describes how data may be deleted by table management functions, and how the audit history can be purged.

Current data may be deleted, but audit history can only be purged on a by-date basis per table, not by individual data-subject. In order to comply with the Article, all relevant history records would have to be purged after the data is deemed no longer required, to be retained was extracted to external storage -which would then be outside the ICM system control

Deletion requires an authenticated administrative user (whether internal or external) to perform. The only way to recover deleted data is by restoration of an archived database backup of the entire system.

Data Monitoring

Customers should regularly test, assess, and evaluate the effectiveness of their technical and organizational measures to comply with GDPR. These measures should include ongoing privacy assessments, threat modeling, centralized security logging and monitoring among others.

The audit logging integrated into ICM provides these capabilities (although in the case of on-premise, synchronising the system time is a computer management responsibility), and the application standard user guide describes this.

Responding to Data Subject Rights

To respond to the customer request:

The user guide describes how to access and manage data via the administration user-interface.

This is covered by the standard user guide. (Training videos are also available via IBM SPM's YouTube channel)