Merative™ Social Program Management

Consent Management

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. Merative 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.

This document is intended to provide guidance to help you in your preparations for GDPR readiness. It provides information about features of this offering, and aspects of the product's capabilities, that may help your organisation with GDPR requirements. 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.

The GDPR and Consent Management

The GDPR states that there shall be at least one lawful basis for processing of data, of which consent is one.

The following are some of the key requirements that may come into consideration in relation to consent management as set out by Article 7 of the GDPR:

- Consent information shall be presented in a manner that is clearly distinguishable from other matters.
- Consent information shall be presented in an intelligible and easily accessible form, using clear and plain language.

If a client chooses consent as their lawful basis for processing of data, SPM contains features and functionality that can be used to help address such requirements.

Social Program Management and Consent Management

SPM contains customisable functionality to support the following aspects of consent management:

- Presentation of consent
- Recording of the consent
- Management of the consent data

During an intake of personal data, a consent page can be displayed so that applicants can agree to allow their information to be used. Consent can cover all processing activities that are carried out for the same purpose or purposes. If processing has multiple purposes, consent can be given individually for each purpose.

Using Intake and the Datastore

A consent page can be written for an organisation by using an IEG script.

During a screening or intake process, a data subject will submit his or her information. The data that is captured during the IEG script execution is persisted in the Cúram Datastore. The Datastore has a public API that can be used in the application code. The API is most often used to retrieve information from a populated schema, but it can also be used to prepopulate a schema.

For example, after a client has completed an online application and provided consent, the client can submit the information in the application. The Cúram Data Mapping Engine (CDME) can then be used to extract the data from the schema and to populate tables in the relational database. CDME reads the data and uses rules from a mapping specification to transform the data into something that is readable by an application builder. An evidence application builder uses a mapping configuration to call on the evidence API in order to create the new evidence entities for the new case.

Note: *Data that has been captured during an IEG script session is stored in the Datastore. If the screening or application that the client was making is not submitted, then the session remains in the Datastore. It is the responsibility of the system administrator to ensure that incomplete IEG sessions are purged from the system at a regular interval. One such batch job that can purge application data is shipped with Universal Access and is called "CitizenWorkspacePurgeNonReferencedDataProcess".*

Using Evidence

Storing consent information as evidence in SPM would require the configuration of a new dynamic evidence type. The evidence type definition might store attributes such as those in the following list:

- Name of the person who is giving consent
- The date on which consent was given
- The category of data that is being consented to
- The processing purpose for which consent was given

As consent management requirements will typically vary from customer to customer, a dynamic evidence type that stores consent information is not included in the product. If required, each customer can design their own custom consent management storage model.

Depending on the requirements of a program that is being offered by an organisation, consent evidence records can be either associated with a person or mapped to an application case for further processing.

The use of IEG scripts is one method of gathering consent. Alternative methods could include modification or development of the UIM screens that are used by caseworkers to capture a client's information. In this scenario, the client's consent can then be stored as evidence on either the client's person or application case.

Further Information

For more information about developing IEG scripts, see the “Working with Intelligent Evidence Gathering” guide.

For more information about developing with CDME, see the “Developing with the Data Mapping Engine” guide.

For more information about configuring dynamic evidence, see the “Configuring Dynamic Evidence” guide.

For more information about developing UIM pages, see the “Cúram Web Client Reference” guide.