GDPR Compliance with Qorus Integration Engine

1 Introduction

This document is based on the EU General Data Protection Regulation (EU 2016/679: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC) which entered force on the 24th of May, 2016 and applies from the 25th of May, 2018 and is binding in the entire territory of the European Union.

Compliance with the EU GDPR can only be guaranteed with appropriate business processes and with IT systems and integration processes designed specifically to support the requirements outlined in this regulation.

Directive EU 2016/680 (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG) is related but is not binding in the territory of the EU without codification with corresponding local legislation.

The design documented here describes changes to Qorus Integration Engine that can be used with appropriate business process and appropriately designed interfaces to achieve compliance with the EU GDPR.

The overriding goal is to allow an organization to meet the EU GDPR's requirements, in particular EU GDPR Chapter IV, Section 1, Article 25: *Data protection by design and by default* provides a fundamental basis for the design documented here, but full compliance cannot be met by changes in the integration layer alone.

In particular, the following (non-exhaustive) external dependencies are not part of this design but must be fulfilled:

- The external identification of *personal data* as defined by EU GDPR Chapter I, Article 4 *Definitions* and Chapter II, Article 9 *Processing of special categories of personal data* must be made in the analysis phase of each change or new development. Interfaces containing personal data must have the personal data clearly identified in advance and detailed information about the location of personal information must be included in design documents, technical specifications and reflected in the test plan. This also includes the description of identifiers used to index personal data as well as metadata associated with this data (the purpose, categories, recipients, and storage rules) so that

personal data can be queried and purged by authorized users to meet EU GDPR requirements.
- The enforcement of access controls and logging to systems storing personal data to ensure that only authorized personnel access such data and that all accesses are logged
- The enforcement of external security policies to ensure that data transfers potentially containing personal data are subject to encryption to ensure that they cannot be read or intercepted by unauthorized persons or systems
- Appropriate business processes that allow for subjects of data collection (customers and partners) to have their data processed or deleted
- The establishment and enforcement of business processes relating to capturing the consent of individuals to have their personal data collected and processed

The design includes the following:
- Changes to Qorus that provide mechanisms by which personal data can be securely received, stored, identified, retrieved, and deleted providing direct support for the following:
  - EU GDPR Chapter III, Section 2, Article 15: *Right of access by the data subject*
  - EU GDPR Chapter III, Section 2, Article 17: *Right to be forgotten*
  - EU GDPR Chapter III, Section 2, Article 20: *Right to data portability*
  - EU GDPR Chapter IV, Section 2, Article 32: *Security of processing*
- Changes to Qorus to ensure that only authorized users or processes can search, retrieve, and purge personal data
- Development guidelines to ensure that personal data are not made visible to external parties through log files, APIs or in raw form while developing a solution that processes such data

NOTE: EU GDPR Chapter IV, Section 5, Articles 42 & 43 provide for the creation of accredited certification bodies at the union level. No such organizations or processes exist at this time; should such a body exist in the future, then Qorus should be subjected to certification at that time if possible.

NOTE: From this point on, personal data will be referred to as *sensitive data* in the remainder of this document.

2 Qorus Changes

2.1 Sensitive Data Storage Solution

Qorus has been be modified to track and manage sensitive data securely and separately from other data. Such data is indexed (with APIs and in the underlying DB storage) with keys

provided that identify the data so that it can be stored, processed, and searched separately from other order data and without exposing sensitive data to unauthorized access.

Sensitive data is be a third type of workflow order data which assumes the roles of both “static data” and “dynamic data”, in the sense that sensitive data can be provided when a workflow order is created, and is also updatable for sensitive data acquired during workflow order processing.

New APIs have been introduced and existing APIs have been extended to handle sensitive data securely.

Sensitive data is stored in an encrypted form in the database, and this data is only accessible by users or processes with appropriate permissions (to be created specifically for this purpose).

Sensitive metadata is stored alongside sensitive data and is free-form data meant to describe the following properties of its sensitive data:

- **PURPOSE**: the purpose of the sensitive data
- **CATEGORIES**: the categories of sensitive data
- **RECIPIENTS**: the recipients or recipient categories of sensitive data
- **STORAGE**: the storage time or rules for sensitive data

Sensitive metadata is designed to support queries by data subjects based on EU GDPR Chapter III, Section 2, Article 15: *Right of access by the data subject*.

Sensitive data identifiers, which are used to index sensitive data, are considered sensitive themselves and are stored in an encrypted form in the database.

In order to allow sensitive data to be processed with non-sensitive data, aliases to sensitive data are be supported. Aliases are not be considered sensitive information and therefore are not stored in an encrypted form in the database.

The database allows for fast indexed access to sensitive data keys and values as well as sensitive data aliases.

2.2 Encryption of Sensitive Data

The encryption is based on symmetric encryption algorithms as follows:

- Sensitive data and metadata: is serialized to YAML and encrypted with AES-256 (https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) using a random Initialization Vector and automatically generated Additional Authentication Data. Additionally, the full Message Authentication Code is stored in the database as well. This offers a high level of security and also ensures that sensitive data is not

exchangeable (i.e. if it is copied in the DB to another order or key, the copied data will be unusable)

- Sensitive data identifiers: are encrypted with blowfish with a 56-byte (448-bit) key and stored in base-64 format in the database. This allows the sensitive data key value (which is treated as sensitive data itself) to be encrypted (or subject to *pseudonymization*) using a secret encryption key and for this value to be used in SQL queries to support fast access or manipulation of the data to support normal processing or user-generated actions (such as queries about personal data stored or to delete / purge personal data stored)

Separate encryption keys for each type of data are used; support for automatic key generation and checks has been implemented.

Because the encryption keys are fundamental to the security of the solution, they must be kept protected and cannot be lost; if encryption keys are lost, sensitive data cannot be recovered.

2.3 External APIs for Sensitive Data Processing

External REST APIs have been developed to allow for sensitive data, metadata, and sensitive data aliases to be:

- Created
- Read
- Updated
- Deleted

It is only possible to perform operations on sensitive data through an encrypted external connection (HTTPS). Any requests involving sensitive data that arrive on unencrypted connections result in an error response to the caller.

External operations with sensitive data are also subject to authorization using new RBAC permissions.

Sensitive data is never be logged in raw form; at most encrypted and base-64 encoded sensitive data values may be logged, which can allow for correlation of sensitive data actions from log files to actual order data to be performed without exposing sensitive data to inadvertent unauthorized access.

External APIs operate on the primary system schema and any archiving schema(s).

2.4 Internal APIs for Sensitive Data Processing

Internal REST APIs have been developed to allow for sensitive data, metadata, and sensitive data aliases to be:

- Created
- Read
- Updated
- Deleted

Internal code is provided sensitive data in its decrypted, raw form. Once sensitive data has been retrieved internally, it can no longer be subject to automatic controls (ex: prohibition of logging), therefore care must always be taken that sensitive data is processed correctly; for this reason Qore Technologies recommends that any interface processing sensitive data be audited for compliance before being allowed to run in a production environment.

2.5 System Job Related to Sensitive Data Purging

A new job has been implemented that will periodically purge sensitive data from the system, independent of any archiving as follows:

- **qorus-sensitive-data v1.0**

This job will purge all sensitive order data from all workflow orders with status COMPLETE or CANCELED from the primary system schema and any archiving schema(s).

In this way sensitive order data can be guaranteed to be deleted from already-processed workflow orders regardless of any archiving schedule or solution.

2.6 System Options Related to Sensitive Data Processing

The following system options has been implemented to support sensitive data processing:

- **sensitive-data-key**: the file name with a 32-byte random key for encrypting sensitive data with AES-256; must be kept secure; must be readable only by the application user
- **sensitive-value-key**: the file name with a 56-byte random key for encrypting sensitive data values with blowfish; must be kept secure; must be readable only by the application user
- **purge-sensitive-data-complete**: if True, then sensitive data will automatically be deleted when a workflow order goes to COMPLETE
- **purge-sensitive-data-cancel**: if True, then sensitive data will automatically be deleted when a workflow order goes to CANCELED

2.7 Executive Summary

Qorus has been updated to allow sensitive data and metadata to be stored with strong encryption and only accessed by authorized users.

The database and system APIs have been enhanced to allow the middleware to support the following actions:

- EU GDPR Chapter III, Section 2, Article 15: *Right of access by the data subject*
  - Sensitive data is searchable and retrievable along with metadata describing the sensitive data and how it is used and stored as required by the EU GDPR

- EU GDPR Chapter III, Section 2, Article 17: *Right to be forgotten*
  - Sensitive data that belongs to workflow orders in **COMPLETE** or **CANCELED** status can be deleted on request

- EU GDPR Chapter III, Section 2, Article 20: *Right to data portability*
  - Sensitive data is searchable and extractable on request in a common format

- EU GDPR Chapter IV, Section 2, Article 32: *Security of processing*
  - Enterprise-class industry-standard strong encryption is used to secure the data; and the system has been designed and implemented so that sensitive data will not be logged or made available to unauthorized parties as long as development guidelines are followed and appropriate business processes are in place to identify and manage the data

Note that design and implementation reviews must be made to ensure that sensitive data is not inadvertently exposed and that the facilities documented here are used appropriately in order to ensure that GDPR-compliant solutions are delivered to production.

Additionally, appropriate business processes must be in place to ensure full compliance with the GDPR; the changes in the middleware cannot be effective in isolation; they can only be effective as a part of an overall commitment from the organization to GDPR compliance.