Quality Management Suite

Regulatory Compliance White Paper

Covering PCS DSS, GDPR, MiFID II and Other Key Regional Regulations

Document Reference
V3.0

Enghouse Interactive
Trevor Davis

1 Change control

Version	Author	Date	Comments
1.0.0	March 2014	Trevor Davis	Initial version
2.0.0	February 2017	Trevor Davis	Updated branding and product description
3.0.0	April 2018	Trevor Davis	Updated to include GDPR

Contents

2 About GDPR

About GDPR

The EU's new General Data Protection Regulation (GDPR) applies from the 25th of May 2018. The Regulation propagates rules relating to the processing and transfer of personal data of a natural person. '**Personal Data**' means any information relating to an identified or identifiable natural person ('**Data Subject**'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. '**Processing; Processed**' means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data and Enghouse software

Enghouse Interactive Software ('**The Software**') may collect and store Personal Data such as phone numbers, email addresses and voice recordings, as implemented and put into production use by Customer. It is the responsibility of the Customer ('**Data Controller**') to ensure that the Processing of such Personal Data is done within the scope of their permitted remit as dictated by Data Subjects and data authorities.

According to the regulation, Personal Data shall be Processed lawfully, collected for specific purpose and limited to what is necessary for that purpose. The Personal Data shall be kept only for as long as it will fulfil the purpose and kept in a manner so as to prevent breaches of such Personal Data. Data retention obligations may further be set by contract, or by regulatory obligations specific to the industry and jurisdiction of the Data Controller, Data Processor, and/or Data Subjects.

GDPR establishes several individual rights for Data Subjects, including but not limited to the right to access and rectify their Personal Data. Enghouse Interactive, as a Data Processor, provides Software and Services that aid Data Controllers in implementing their own environment of data privacy and data security to comply with GDPR requirements, including the ability to search, delete and export Personal Data as the Data Controller may find necessary in accordance with an exercise of an individual right by a Data Subject.

Scope

This Enghouse Interactive software package may include tools, documents or guidelines intended to assist an organization using the software on their journey to achieving GDPR compliance across the business.

DISCLAIMER

TO THE EXTENT ENGHOUSE INTERACTIVE IS PERMITTED BY LAW TO LIMIT ITS LIABILITY, THE SOFTWARE PRODUCTS AND THIS DOCUMENT ARE PROVIDED BY ENGHOUSE INTERACTIVE, AND ACCEPTED BY THE RESELLER PARTNER / CUSTOMER "AS IS" AND ENGHOUSE INTERACTIVE GIVES

TO THE RESELLER PARTNER / CUSTOMER, NO OTHER REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT, THE PRODUCT(S) AND/OR THE PERFORMANCE OR RESULTS OF USE THEREOF, ARE, IN ANY WAY, COMPLIANT WITH GDPR REGULATIONS AND THE RESELLER PARTNER / CUSTOMER HEREBY UNDERSTANDS AND AGREES THAT IT IS THE RESPONSIBILITY OF IT OR ITS SYSTEM INTEGRATOR PARTNER, AS PART OF THEIR CONTRACT WITH THE CUSTOMER, OR THE CUSTOMER'S COMMITMENT AS PART OF THEIR GDPR POLICY, TO ENSURE THAT THESE LEGALITIES ARE MET.

Support of Enghouse Interactive Software with reference to GDPR

Enghouse Interactive supports The Software via its standard support agreements and SLAs. These agreements are definitive in determining if and how issues are resolved, and Enghouse Interactive does not make any warranties or representations to the adequacy, sufficiency of any kind, expressed or implied, including, but not limited to, the completeness, correctness, performance, merchantability, currentness, and fitness for a particular purpose, whether error-free or uninterrupted, and provides no guarantee that The Software meets or will meet the customer's requirements, whether arising by usage of trade, course of dealing or course of performance. Any issues raised (including those relating to management of personal data) will be handled via the standard response and resolution processes as defined within those agreements.

3 Executive Summary

International regulations that are designed to provide organisations with a set of statutory obligations with respect to personal data protection have been in force for many years. These regulations continue to be updated periodically as events and new technology precipitate change. Recent examples are the raft of new regulations that emerged after the 2008 financial crisis, and the General Data Protection Regulation (GDPR) governing personal data management, largely in response to advances in software, Cloud and social media platforms, data mining and data storage technologies.

This White Paper describes the QMS product and the features within the product that can help organisations meet their regulatory needs. It covers two regulations in detail: the Payment Card Initiative Data Security Standard (PCI DSS) and GDPR. Other regulations are listed for reference. Generally, the features consistent with meeting PCI DSS and GDPR regulatory obligations are also suitable for other regulatory standards; however, organisations should make their own assessment according to their individual needs.

It is important to note that no call recording system is itself regulatory compliant. There are no benchmark certifications available from any regulatory body. For example, it is not possible for a call recording vendor to go to the PCI DSS regulatory body and request certification for their call recording product. Instead, call recorders are developed with the features required to enable companies to demonstrate that their call recorder conforms to their overall compliance strategy and adheres to regulatory standards where needed. It is the responsibility of individual organisations to ensure that their business practices and business systems allow them to meet any applicable industry regulations.

This document does not provide professional legal advice. Actions or decisions should not be based solely on this document. The regulations discussed here are broad and cover all aspects of an organisation's policies and procedures, whilst this document is restricted to how those regulations apply to call recoding systems only. If in doubt, you should obtain independent legal advice.

3.1 Quality Management Suite Product Overview

Quality Management Suite (QMS) is a suite of call recording and quality management applications designed to provide organisations with robust, secure and dependable recording of inbound, outbound and internal communications. QMS records IP-PBX, such as Skype for Business, Cisco, Avaya, NEC and Mitel, as well as SIP environments. It is designed to record as an extension-side recorder and is particularly suited to the small to medium contact centre market.

QMS consists of a number of integrated components that can be deployed individually or in combination.

1. Audio recorder for VoIP environments
2. Screen recorder can be deployed together with voice recording, to provide corresponding details of desktop activity
3. Text (IM, chat, email) recorder for the capture of text-based communications

4. Agent evaluation for quality monitoring of contact centre staff

3.2 Summary of Key Regulations

1. Payment Card Initiative Data Security Standard (PCI DSS). All firms who handle, transmit, store, or process information concerning credit or debit payment cards, or their related card data, are required to be compliant with PCI DSS regulations. This is a global standard.
2. General Data Protection Regulation (GDPR). This EU regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.
3. Financial services regulations include national and multi-national regulations including:
    a. Markets in Financial Instruments Directive (MiFID II) is a European standard designed to offer greater protection for investors and inject more transparency into all asset classes: from equities to fixed income, exchange traded funds and foreign exchange.
    b. Dodd-Frank Wall Street Reform and Consumer Protection Act is a USA law that regulates the financial markets and protects consumers. Its eight components are designed to help prevent a repeat of the 2008 financial crisis.
    c. Financial Conduct Authority is a financial regulatory body in the United Kingdom, but operates independently of the UK Government.
4. Health Insurance Portability and Accountability Act (HIPAA). This regulation offers protection to Americans with health insurance coverage, along with the security and privacy of their health data.
5. Medicare Improvements for Patients and Providers Act (MIPPA) requires health care marketers to record their conversations to prove that they are not participating in deceptive or high-pressure tactics. In addition, the September 18, 2008 update to the Medicare Marketing Guidelines state that all appointments made via telephone with current or potential Medicare subscribers must be recorded in order to document the interaction.
6. Centre for the Protection of National Infrastructure (CPNI). An American standard that protects American national security, covering physical security, personnel security and cyber security/information assurance.
7. Statement on Auditing Standards No. 70 (SAS-70). Developed by the American Institute of Certified Public Accountants, this is a standard that covers a firms control objectives and control activities, which often include controls over information technology and related processes.
8. ISO 9001. This is by far the world's most established quality framework, currently being used by over 1m organisations in 178 countries worldwide, and sets the standard not only for quality management systems, but management systems in general.

4 PCI DSS

The main areas of PCI DSS compliance that affect call recording are listed below. Further information can be obtained from the PCI Security Standards Council's information supplement, March 2011, entitled Protecting Telephone-based Payment Card Data.

1. In general, no cardholder data should ever be stored unless it is necessary to meet the needs of the business (generally restricted to a legislative or regulatory obligation).
2. Sensitive data on the chip or magnetic stripe must never be stored after authorization. If an organisation stores the primary account number (PAN), it is crucial to render it unreadable (see PCI DSS Requirement 3.4). Organisations also must comply with Requirements 3.1 through 3.6 of the PCI DSS with respect to protection of stored data. Note: Encrypting sensitive authentication data is not by itself sufficient to render the data unreadable.
3. Limiting the amount of time that card information is kept on the recording server. It may be necessary for corporate governance, legal and QA departments to work out a compromise between what is needed to adhere to the PCI DSS and other regulatory compliance requirements.
4. Never allow the card validation code (referred to as CAV2, CVC2, CVV2, or CID) to be stored in a digital audio or video format (e.g., WAV, MP3, MPG, etc.). If the recording system cannot block the audio or video from being stored, the code must be deleted from the recording after it is stored.
5. Protect stored cardholder data. Stored data should be kept to a minimum. A policy for retention and disposal should be in place. All customer data should be stored using strong encryption.
6. Encrypt transmission of cardholder data across open public networks. Protocols such as secure socket layer (SSL) and transport layer security (TLS), or internet security protocol (IPSec) must be used for the transport of data across open public networks.
7. Restrict access to cardholder data. Access to cardholder data should be limited to those individuals whose job requires access to the information.
8. Assign a unique ID to each person with computer access. This ensures, with the appropriate audit capabilities, that each person can be held accountable for their actions.

The following table gives a summary of the PCI DSS guidelines for cardholder data elements:

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data*	Full Magnetic Stripe Data†	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/ CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

4.1 QMS's Implementation of PCI DSS Standards

Implementing a call recording system into a PCI DSS compliant contact centre requires a review of all relevant business processes to ensure full compliance. The following features are designed to help organisations meets their requirement obligations but they must be considered in context of other systems and procedures in place within the organisation.

1. Primarily QMS contains features designed to help prevent the recording of credit card data, whilst allowing for the recording of the remaining parts of the call. There are a number of trigger options allowing for both manual and automatic suspension of recording for both audio and screen recordings. The trigger options include:
    a. Manual pause and resume via the recorder interface.
    b. Manual pause and resume via the Desktop Utility.
    c. An XML app for compatible handsets that provide an manual pause and resume option on control keys on the handset.
    d. API methods for pause and resume that can be triggered via external systems, for example a payment gateway.
2. QMS contains an automatic deletion process that removes recordings and associated metadata that have exceeded a predefined retention period. The deletion process can be set individually for audio, screen and text messages. Additionally, retention policy can be applied at an individual group level, meaning that different policies can be defined for PCI compliant recordings and other recordings not governed by PCI. Additionally, designated administrators can be granted with the ability to selectively delete recordings. This type of deletion creates an audit log event listing the user, date, time and action taken. These features allow companies to define and maintain a data retention and disposal policy.
3. The storage of all recordings in QMS can be encrypted using 256-bit AES encryption, an industry standard strong cryptographic protocol. This helps to protect sensitive data that is permitted for storage. QMS can encrypt universally, be set to not encrypt new

recordings, re-encrypt recordings with a new key and decrypt recordings through the use of an authorised account. The encryption key is a dual key model that provides two separate people with key fragments so that no one individual has full key access. During the creation of an encryption key the QMS suite requires these two people (who require Administrator accounts) to be simultaneously logged into QMS in order to generate the key. It is recommended that the key is periodically changed, for example annually.

4. The QMS interface supports SSL sessions. When enabled user access to the interface is always encrypted, ensuring that data transmitted from the recorder via the interface is secure when transmitted across open public networks. Additionally, the inter-service communication between different components of the recorder are also encrypted so that, in the event that the components are split across network segments, all inter-service communication is also secured.
5. Access to QMS can be tightly controlled and maintained by the primary system administrator and other administrators granted permission from this root account. This account has full access to the QMS recording features. Account types can be restricted to view only a subset of the lines being recorded and what QMS features are available to them. For example, a user account can be restricted to access a single line that is operated only by that user. User accounts can also have restricted access to functionality, for example by removing permission to playback recording, delete recordings or export recordings. Each account is audited by QMS when it logs on, requests playback, deletes a recording, and conducts other tasks within the recorder.
6. It is expected that each user who requires access to the recorder is provided with a unique account ID.

5 GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) applies from 25th May 2018.

GDPR was designed to protect and empower all EU citizens data privacy. Two purposes of the regulation were to harmonize data privacy laws across Europe and to adapt those regulations to recent technology changes.

Prior to GDPR every EU country had their own national law. Companies and organisations that already adhered to these national laws will be well prepared for GDPR but some key changes are as follows:

- Data Processors (a person or organisation that processes personal data) will be governed by new obligations and an extended personal responsibility for protection of personal data. The Processors will in many cases have the same obligations as the Data Controller (legal person).
- Data protection officers are required for companies with more than 250 employees.
- The consent for storing personal data will be strengthened.
- Extended rights for citizens to obtain personal data concerning them and the right to have that personal data erased.
- Increased protection for children.
- Higher penalties for non-compliance.

Call recording is a form of data processing and is an important application to consider within the context of GDPR because recordings can contain sensitive personal information such as banking or financial details, health information, family details, religious beliefs, sexuality, etc.

Individual regulations within countries have governed the circumstances under which organisations can record calls and what notices are needed for employees and customers when recording is taking place. GDPR implements much stricter rules. Firstly, there are only six specifically defined circumstances under which organisations can record calls.

1. The people involved in the call have given consent to be recorded
2. Recording is necessary for the fulfilment of a contract
3. Recording is necessary for fulfilling a legal requirement
4. Recording is necessary to protect the interests of one or more participants
5. Recording is in the public interest, or necessary for the exercise of official authority
6. Recording is in the legitimate interests of the recorder, unless those interests are overridden by the interests of the participants in the call

For organisations operating under UK law prior to GDPR, for example, assumed consent on behalf of the customer was a satisfactory condition for call recording. Under GDPR regulations explicit consent has to be obtained.

Organisations wishing to record customer interactions will have to maintain a documented call recording policy that specifies which of the six conditions apply to them and what measures are being taken to obtain the consent of third parties. The policy will also need to document policies and procedures for protecting recordings from misuse. Additional, attention needs to be given to the use of an organisation's phone system by members of staff for personal calls. Calls recorded in this circumstance are liable to be in breach of GDPR.

5.1 QMS within the GDPR Framework

This section describes the data areas of the product where personal information may be stored, and the product features that allow for the identification and retrieval of specific information. The section is divided into four areas:

1. What kind of personal data could be stored in the QMS databases and where it would be stored.
2. How to search and identify data related to a specific person for the purposes of Right to Information.
3. Options for dealing with consent and non-consent to retain recordings.
4. Options for dealing with legitimate requests for records to be deleted for the purposes of Right to be Forgotten.

5.1.1 Storing of Personal Data in QMS

All data that can be used to identify a person is defined as Personal Data and is subject to the provisions of the General Data Protection Regulation (GDPR). This section details the areas of QMS that store data that may be considered as Personal Data, however it is the responsibility of the organisation using QMS to decide whether or not data is considered as Personal Data according to GDPR.

1. The QMS database, based on Microsoft SQL Server, contains metadata for each recorded interaction. The media type of that interaction will determine the specific data stored within this metadata record. The following Personal Data fields may be populated:
    a. Phone number – for audio calls.
    b. Caller line identification (CLI) – only if the data is presented in the SIP header.
    c. Email address – captured only if email recording is active.
    d. Name or user ID – captured only if IM or chat recording is enabled.
    e. Comment – manually input by a call handler or manager during or after the call and possibly containing personal data.
    f. Flag – manually or automatically assigned during or after the call and possibly containing personal data.

2. The QMS file store contains call recordings that are available for search and retrieval. The recordings may be of audio, screen, or text or interactions depending upon the media capture methods that have been licensed and implemented on QMS. The recordings are likely to contain personal data.
3. Log files contain system information to enable troubleshooting and traceability. The log files are stored in the file system on the QMS server. Personal data contained within logs files is limited in nature and restricted to call identifier data. No log files are written to external systems, although it is possible to monitor logs files using a SNMP system. Log files are periodically removed from the system during standard housekeeping processes. The standard retention period is 30 days.

5.1.2 Retrieval of Personal Information (Right to Information)

If an organisation receives a request to describe what personal information it holds for a particular customer one of the systems that would be queried is QMS. QMS provides an easy set of steps to list records stored for a particular customer provided one or more of the personal data identification fields are populated.

To do this an authorised user would utilise the Recordings interface of QMS, enter appropriate filter criteria and run a query to retrieve all relevant records. The resulting record retrieval can be viewed within the interface, or exported in CSV format.

QMS also supports data retrieval via API for those organisations who wish to automate this process via third party systems.

5.1.3 Consent

One of the stipulations of the GDPR regulations is that explicit consent must be obtained, unless other regulatory requirements overwrite that. It is the responsibility of each organisation to implement a suitable method for obtaining and registering consent and withdrawal of consent. A possible method is to utilise an IVR to capture this. The third party is asked to select a specific option to avoid call recording and the call is routed to a line group that is excluded from recording. QMS can support this and similar scenarios through the use of call recording profiles that determine under what conditions it is appropriate to record. Multiple profiles can be created to manage more than one scenario.

It should be noted the QMS is always deployed in such a way that it has no access to the primary call path and therefore cannot influence call routing or pick-up messages. It is the responsibility of other applications to handle these functions.

5.1.4 Right to be Forgotten

The majority of companies have a legitimate right, and in some industries a mandatory requirement, to record calls to and from third parties, which override the GDPR regulations. Examples are provided in the introduction to section 4 above.

The QMS system also has call deletion rules and housekeeping processes that remove data periodically after a defined time period. The default for call retention within QMS is 365 days, although this can be overwritten at system level, or for any defined group, to meet the specific requirements of an organisation. For example, the MiFID II requirements stipulate a five-year retention period and this can be defined within QMS provided sufficient storage is available. The removal of recordings also deletes the associated metadata from the QMS database.

As mentioned previously, housekeeping tasks periodically remove old log files from the system. QMS supports the archival and exporting of information. Once information is extracted from QMS using these methods it moves outside of the jurisdiction of QMS and organisations should implement separate polices for managing this data.

In some circumstances, organisations may determine that a request by a customer, or other third party, to remove personal data is legitimate and that data needs to be manually removed from QMS. Only designated administrators have the appropriate access to the deletion options within QMS, but assuming a user does have these permissions then a simple query to list all records associated with the third party will retrieve the appropriate data and these records can then be selected and deleted using the Delete option within the Recordings interface. A log is written whenever records are manually deleted from QMS that lists the user who performed the deletion, plus the date and time. An API method can also be used to automate selected deletion from a third party system. The deletion request removes all selected records, both the physical recordings and the associated metadata. Organisations who backup the recordings file store and database may need to determine a separate procedure for removing data from these backups.

6 MiFID II (And Other Financial Service Regulations)

The following section relates primarily to MiFID II, a comprehensive set of regulations implemented by the European Union that cover the European financial services sector. The resultant call recording functionality is applicable within many other financially regulated markets.

The Markets in Financial Instruments Directive (MiFID) is a European Union legislative framework for governing the financial sector within Europe. Initially implemented in 2007 the directive governs investment services provided by investment firms and banks as well as financial trading within stock exchanges and other trading vehicles.

An updated framework, known as MiFID II, has been implemented following shortcomings in the original specification that became evident after the 2008 financial crisis. The implementation timeframe for this is, at the time of writing, is as follows:

- The regulations came into force on 3rd January 2018;
- Regulated firms have two years from this date to implement appropriate systems and demonstrate compliance.

The regulations place increased responsibility on firms to record and securely store communications with their clients. Interactions with clients must be recorded and stored using the following guidelines:

- Conversations must be recorded when either instructions are confirmed with clients, or when advice is given to clients.
- The conversation must be recorded regardless of the medium used, i.e. whether it was a telephone or mobile phone call, an email instruction, some other electronic form of communication, or a verbal, face-to-face instruction.
- Records must be kept for a minimum of five years.

This section provides details about the MiFID II regulations as they relate to call recording and details the solutions that Enghouse provides to help regulated firms meet their compliance needs. These include:

- Call recording systems designed to meet financially regulated market needs;
- Secure storage for recordings including industry standard encryption and digital watermarking technologies;
- Configurable retention policy;
- Secure access control on to the recording system;
- Audit logs of user access and usage within the system;
- Compliance with PCI DSS standards;
- Security within the user interface with support for SSL certificates.

6.1 QMS's Regulated Market Features

1. The ability to define a minimum retention period of 5 years with the ability to create traceable archives.
2. Recordings are encrypted using 256-bit AES encryption, an industry standard strong cryptographic protocol. An authorized account is required to decrypt and playback the calls.
3. QMS's interfaces support SSL sessions. When enabled, user access to the interface is always encrypted, ensuring that data transmitted from the recorder to the user is secured when transmitted across networks.
4. User access is both audited and controlled through a multi-tier account structure. System administrator accounts provide a means to create and manage access policy for user accounts by allowing security profiles to be defined and user accounts to inherit a security policy.
5. Other system tasks are also audited at a user level, for example playback, export of recordings, failed login and deletion requests.
6. User authentication can be linked to a single sign-on strategy.
7. The notification to call participants that a call is being recorded must be implemented externally to QMS, e.g. by the PBX, principally because the recorders are passive and have no call control ability.
8. Each recording has a digital watermark attached to demonstrate authenticity. MD5 is used to apply this.
9. Text communications can be recorded by QMS using either API methods or customised integration into the text communication platform.

7 Other QMS Encryption and Security Details

7.1 Recording Encryption

The initial encapsulation of media as a call is in progress and is being captured and written to disk by QMS is in unencrypted format. This temporary file is converted to an Opus or MP3 file at call termination, encrypted using the key phrase and a unique MD5 hash is applied. The encrypted file is then moved to permanent file storage and any temporary files are destroyed immediately after processing is complete.

7.2 Applying a New Encryption Key

The QMS Admin interface provides a method for revoke existing keys and applying a new two-part key. The re-encryption process will be performed as a background task and may take some time to complete, depending upon the quantity of recordings to be reprocessed.

7.3 SSL Security

QMS SSL support uses Microsoft WCF services that provide a number of security options. For example it is possible to force SSLv3. QMS has no support for OpenSSL.

7.4 Distributed Environments

The QMS DataService manages all remote CallRecordingServices and the associated SSL encryption keys via the Windows WCF service. The connection between the DataService and the CallRecordingService is then secured via SSL.