OFFICEMASTER CALLRECORDING

Installation and configuration of OfficeMaster CallRecording according to MiFID II requirements

Best Practice |2017/21/06

Ferrari electronic

Table of Conent

Ferrari electronic

1. Configuration of OM CallRecording

This document serves as a best practice to clarify which components and settings of CallRecording have to be used and adjusted in order to fulfill all MiFID II requirements. Furthermore, it provides background information and refers to adjustments, which are not part of the actual OfficeMaster CallRecording – solution, but are nonetheless crucial for a MiFID II- compliant usage (e.g. compliance).

1.1. Configuration Password

In the first instance it is essential to set up a password for the configuration interface to prevent unauthorized access and manipulation.

1.2. Automatic over On-demand Call Recording

The basis of any legal solution

An automatic call recording solution tapes inherently every call automatically and does not need to be started each time manually unlike an On-demand call recording system. The risk that comes with any On-demand call recording solution regarding legal requirements is obvious: Since in the end it is the user who initiates the record, this method is prone to manipulation and failure. These dangers are eliminated by using an automatic system which takes the responsibility for the starting the record from the user.

1.3. Define Prefilter, Comply with data Protection law

MiFID II vs. data protection law

At this point the MiFID II obligation to record calls on one side clashes with the data protection law on the other side, which prohibits phone taping. Although MiFID II specifically demands to record certain calls, the data protection law restricts these demands concurrently. It is essential to adjust the call recording system in a way to comply with both laws. To set up so-called “prefilter” is a crucial part in doing so.

Use of prefilter

Prefilter allow to define which ports are being recorded and at what time. Furthermore, they offer the option to preclude certain numbers from being recorded a priori. This is of importance, for example, when dealing with calls from or to work councils, legal department or if there are fixed times when a particular port is only used for calls that MiFID II does not apply to.

Note! It is obvious that even after the most accurate configuration of any call recording system, the legal requirements regarding the demands and prohibitions can only be met if all staff in question have been briefed in depth. Therefore, MiFID II explicitly demands such briefings regarding compliance aspects.

1.3.1. Culture of Compliance

Plan processes, identify scenarios, find solutions

The usage of any call recording solution requires in addition to a deeply briefing of staff, some well-structured organizational and control arrangements. This happens to be necessary due to the above mentioned interplay of demands and prohibitions.

Initial situation - The three kinds of calls:

1. Those, that have to be recorded from the outset
2. Those, that are clear to not be allowed to be recorded from the outset
3. The unknown ones, which status can not be clarified before the actuall call happens

Those calls from group 1 and 2 can be administrated through prefilters and will be automatically recorded respectively not recorded.

It is incidental that the most problematic group is the third one, in which the actual status of the calling party can not be clarified before the actual conversation. Therefore, creating a failover-solution seems so to be crucial:

- Unknown calling parties will be forwarded to a secretary in order to make sure MiFID II demands do not apply to this conversation and therefore the call does not have to be recorded.
- Phone numbers of brokers in question are only given to clients that have already been informed about the requirement of call taping.
- The telephone system could be configured in a way that unknown calling parties receive an announcement that informs them about the recording. Since the EU demands this information to be in the language that is also used for the contract negotiation with the client in question, this solution appears to be unpractical.

1.3.2. Internal Calls

Depending on the substance of a call, it can be required to also record a company‘s internal conversation. As in most cases these kind of calls are encrypted (e.g. Skype for Business) they cannot be recorded without prior adjustments. Therefore, internal calls, that need to be recorded, have to be redirected through the PSDN first. This aspect also requires a briefing of staff.

1.4. Set up the Collector Service

Record without limit of storage and administrate different locations

By setting up the collector service, the request for a high performant and extensive call recording solution is met by forwarding saved data to a network share.

This offers two advantages:

- At first all recordings are being saved locally. To prevent having a recording-stop due to the reach of the maximum of local storage capacity, those files are being sent to a network share and saved for good whereas the local storage can be overwritten after a defined amount of time or storage to ensure an unlimited recording capacity.

- Furthermore, the collector service allows to administrate multiple sites all over the world. This keeps administrating costs low as at the same time it provides a higher level of security for all saved files.

1.5. Encryption

Protect files

The EU requests that all stored files have to be encrypted. Thus it is mandatory to set a password for .wav-files in the OM CallRecording configuration interface.

1.6. Format

Prepared for the future

MiFID II request a future-proof data format to ensure the authorities in question are able to evaluate them. OM CallRecording saves in .wav format by default. This guarantees that those files can be read by any audio player and easily be converted into other formats if necessary. By choosing different levels of quality, it is easy to adjust the size of each recorded file.

2. Configuration of Call Monitor

The call monitor is the software component of the recording system. To completely comply with all MiFID II requirements, it is crucial to adjust some settings of the call monitor as well.

2.1. Main Password

Who has access...?

In the first instance it is essential to set up a password for the administrative program to prevent unauthorized access and manipulation.

2.2. Restricted User Interface

...and in which scale?

This allows to protect definable functions by password (e.g. play, delete, send...), which reduces the hazard of maloperation and manipulation.

Note! If the system is supposed to be used by various people with different administrative rights, the main admin can hereby restrict the rights of other users.

2.3. Fingerprint

Manipulations leave fingerprints

The fingerprint function meets the MiFID II demand to trace manipulation. This functions is activated by default and shows every time the file is used a little symbol that clearly indicates whether the file has been manipulated or not.