MirrorWeb

A GUIDE TO

Electronic Communications in MiFID II, Article 16

mirrorweb.com

Contents

Introduction

Even with MiFID II implemented, many firms are still struggling with the extent of their responsibilities in order to comply with the updated legislation.

One particular aspect of the legislation that has proved difficult to interpret is Article 16, regarding recording electronic communications - the main confusion of which, is defining what *"electronic communications"* are.

IN THE REST OF THIS GUIDE:

- Find out what needs to be recorded under the umbrella of electronic communications
- Understand the most effective way of recording and retaining electronic communications
- See how our solution will help firms achieve compliance in accordance with the Directive

A Summary of MiFID II, Article 16

Compared to its predecessor, Article 16 of the MiFID II Directive includes much stricter rules where electronic communications recording is concerned and what safeguarding firms are required to undertake going forward:

ARTICLE 16(7) STATES:

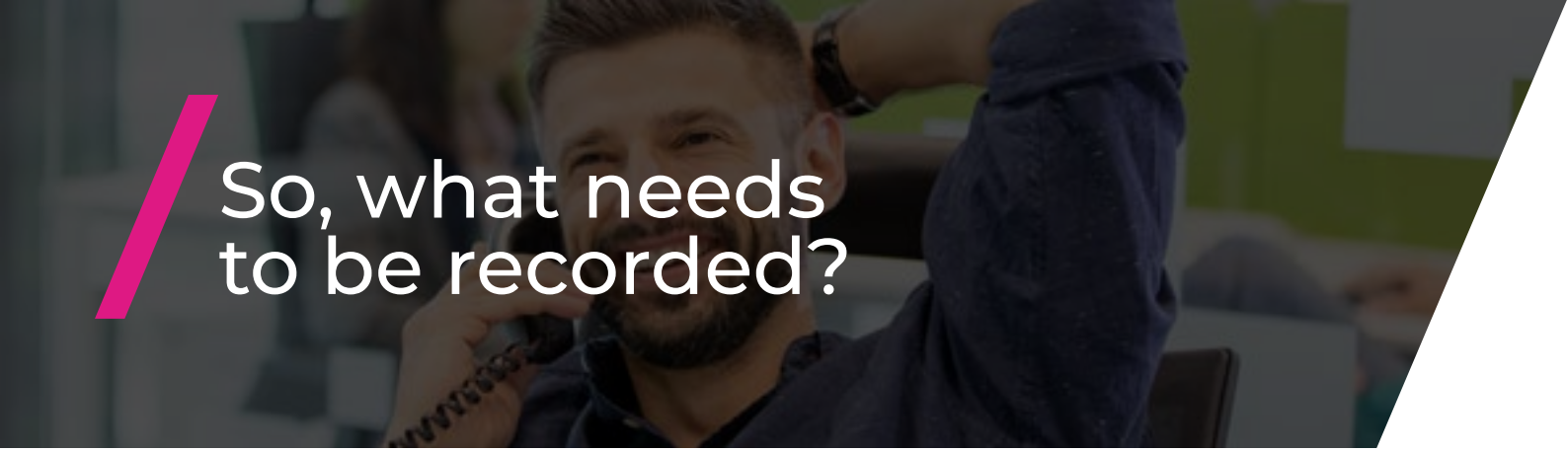
"Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders."

IT GOES ON TO SAY:

"Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services."

Firms are required to keep a record of all communications that conclude in a sale or intended to result in a sale. In addition to this, firms are also legally obliged to keep a record of these communications for up to seven years (dependant on local regulation requirements).

The complex and ambiguous nature of the Directive, as well as the scale of what is required, has resulted in much confusion in the industry. In this guide, we'll be looking at Article 16 and electronic communications in depth and provide more clarity on what firms need to be doing in order to comply.



So, what needs to be recorded?

When it comes to defining “electronic communications”, many make the mistake of thinking this just consists of emails or the firm’s website.

However, electronic communications can consist of more than just what you handle within your estate (such as a website) and include third party platforms like social media accounts.

Here is what we have defined as falling under the *“electronic communications”* umbrella:

- Websites
- Blogs
- RSS feeds
- Emails
- Social media accounts
- Instant message
- SMS/MMS
- Chat
- Videos

Through our conversations with firms in the finance industry, it's become very clear just how little the practical understanding of Article 16 is due to the ambiguous nature of the language used.

We found most firms assumed that website backups and third party platforms could be defaulted to as a compliance measure but that is simply not the case.

How can you be compliant with Article 16?

Now that MiFID II has come into effect, firms are legally required to capture and store electronic communications in the pre-, during and post-trading phases of their business' transactions.

It is likely that, as each firm is different, a varying combination of electronic communications may be employed. Therefore in order to understand what you are required to record, the first stage is to review all electronic communications that your firm uses and understand what recording processes you already have in place for each.

This stage is particularly important in identifying any gaps within your current infrastructure that you need to address immediately.

The next stage is to understand that all captured records of communication must be *"complete, quality and accurate"* if they are to be compliant with the Directive.

We've defined these terms below in more detail to help you understand what a regulator will be expecting when reviewing your recorded communications:

- **Complete** - The organisation will understand and know all types of electronic communications that are used and by whom. Additionally, they will have a system and processes in place to capture and retain the records of those communications.

- **Quality** - The organisation will be able to reproduce records of electronic communications in their *"original form".*

- **Accurate** - Organisations will be fully confident in the recorded electronic communications' content and metadata that shows the exact times and dates that anything took place.

The best execution for achieving the capture and storage of your electronic communications that are *"complete, quality and accurate"* is by implementing a fully automated and certified archiving solution for your firm.

Why a backup isn't legally admissible

"But aren't we already archiving with backups?"

If your firm is backing up your electronic communications such as your website, you may assume that this is both legally admissible and compliant with MiFID II, Article 16.

There is often a misunderstanding between the definitions of a *"backup"* and an *"archive"* - and where the law is concerned, this is a disconcerting issue.

"What makes evidence inadmissible in court?"

Whilst anything can be considered as evidence, when it comes to MiFID II, other legislation and regulatory bodies, the rules are more strict for regulated firms and organisations.

- **Backups** - Backups are used for operations recoveries. So, if you've deleted, overwritten or corrupted a database you can easily recover it and protect the integrity of your data.

- **Archives** - An archive is a stored version of data that is unchanging and that cannot be changed.

And this is where the difference lies. A backup is able to be manipulated in a number of ways in order to change what's been recorded - which is why a backup is not legally admissible in court because it could be argued that it is refutable. Furthermore, this also means that, according to MiFID II, Article 16, a backup would be non-compliant because the information would not be seen as being *"accurate"* or *"quality"* data.

On the other hand, using an archive that is ISO accredited and uses *"write once, read many"* (WORM) and time stamped functionality, will ensure that the recorded information is fully compliant with the Directive.

Therefore, if you're only backing up your electronic communications, then you need to identify the right archiving solution for your firm and work to implement it quickly.

Why you can't rely on third parties

As electronic communications include things like websites and social media, it is likely that you will be using a third party provider or platform for these services.

For example, your website may be hosted on Wordpress and your social media accounts would be hosted on the relevant social media platforms (Twitter, Facebook, LinkedIn etc.)

However, in accordance with the FCA's guidance on social media and customer communications (FG15/4)[1], it explicitly states that:

"Firms should not rely on digital media channels to maintain records, as they will not have control over this: social media in particular may refresh content from time to time, with the consequent deletion of older material."

[1]FG15/4: Social media and customer communications - FCA

Therefore, firms need to be responsible for keeping an adequate record of any significant communications for the purpose of dealing with claims or complaints effectively. So, if you've been under the impression that you would be able to request records of your electronic communications from third parties, you'll need to rethink your approach. You'll want to ensure that the archiving provider you choose will be able to handle archiving the communications that are held on third party sites and platforms, whilst making certain that the archived records are fully compliant and admissible.

What to do next: A checklist for Article 16

With MiFID II implemented, the majority of firms will have already made assessments of their organisation and policies and have identified which areas are required to comply with the new recording rules.

However, the FCA[2] has recognised that, due to the scale of what is required for MiFID II compliance, they will act *"proportionately"* for those firms who have not yet met the requirements. Therefore, the regulator will be looking more favourable on firms which have been making an effort to comply compared to those who have not made any real attempt or where obligations have been ignored.

[2] A Better View | FCA. 20 Sep. 2017

With this in mind, even if you've already started your review process, we've formulated a checklist to break down what needs to be assessed and what needs to be put into place in order to achieve compliance as soon as possible:

- ☐ Ensure you have an assigned compliance officer/manager who conducts the annual recordkeeping review

- ☐ Look at your organisation's current processes of recording information and report on:
  - What electronic communications your organisation uses where it results in, or could result in a trade
  - If you are only backing up your electronic communications
  - What electronic communications you currently record
  - What electronic communications you need to start recording
  - Whether your records are legally admissible and compliant

- ☐ Lengthen the retention period according to new MiFID II rules and local regulatory requirements (up to seven years)

- [ ] Look into a managed archiving solution and think about:
  - How and where data will be stored
  - If the archives are unchangeable or on WORM (write once, read many)
  - Whether it requires on-premise infrastructure/training
  - You are able to manage your archives in any way
  - You can request archives on demand easily as and when you need them
  - There are strongholds in place in case of system failure
  - What investment is required for the solution

- [ ] Create written implementation policies for your organisation's electronic communications use, retention and surveillance

- [ ] Regularly review and ensure policies have been implemented, are effective and adhered to

- [ ] Start archiving your electronic communications according to your newly implemented policies in compliance with MiFID II, Article 16

- [ ] Aim to be fully compliant with Article 16 in an ongoing process with your archiving solution

Conclusion

In order to demonstrate best practice for MiFID II, Article 16, your firm requires a full archiving solution to start recording your electronic communications effectively and compliantly.

Even if your firm is still not fully compliant at this stage, in using the checklist provided, you can at least ensure that you will be taking the right steps in an attempt to comply as soon as possible.

For more information on archiving for MiFID II, Article 16, request a trial archive of your business' website today and see how MirrorWeb can help with your organisation's compliance.

FREE TRIAL ARCHIVE

MirrorWeb

e: info@mirrorweb.com
t: 0800 222 9200
www.mirrorweb.com
Find us on