dubber | Solution certified for Microsoft Teams

Compliant Calls & Conversations for Microsoft Teams

End not knowing

Solving Compliance on Microsoft Teams

Suppose your business is currently using or thinking about making the switch to Microsoft Teams. In that case, it shouldn't mean compromising the compliance standards you set out to achieve or mean you need to spend materially more.

Unified Call Recording platforms are purpose-built to empower compliance certainty despite the challenges of remote workforces with an increasing number of communication solutions.

Despite organisations spending up to 4% of total revenue on compliance costs, the fines for non-compliance can be significant. Unified Call Recording (UCR), together with voice AI, can enable businesses to capture all call data required by GDPR, PCI DSS, Dodd-Frank, MiFID II, and more. UCR empowers businesses to respond to regulatory requests in real-time, set alerts for potential compliance breaches, and capture, access, and retain conversations in line with privacy requirements and policies.

End not knowing by reading this guide:

This guide will show how to create a secure, compliant and scalable system of record for every conversation – across Microsoft Teams and every communication channel in your business.

Read on to learn more about call and conversation compliance and what to look out for before choosing the right solution for your needs.

The cost of non-compliance can take the form of:

- Business continuity disruption
- Revenue and productivity loss
- Fines and settlement costs
- On average costs equate to 2.71 x the cost of compliance.

Today's Compliance Challenge

On-premise and hosted recording solutions aren't viable post-COVID

With Microsoft Teams reaching 115 million daily active users, and allowances from regulatory bodies made for home workers during the onset of COVID no longer in place, the need for a unified approach to communication capture has never been more urgent.

> **"As organisations raced to deploy communications platforms such as Microsoft Teams they faced new pressures to ensure that communications across these channels were in compliance with industry regulations. This has shifted the requirement for call recording from being application-specific to the need for Unified Call Recording – due to the need to capture every endpoint."**
>
> *– James Slaney, COO*

Businesses need to record their Microsoft Teams calls for various compliance reasons:

- Limit liability
- Resolve disputes
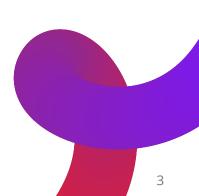- Provide evidence of transactions & trades

These are a few meaningful examples.

Firms will also need to account for data sovereignty and the ability to meet surveillance and reporting requirements. With the cost of compliance increasing by over 60%, businesses are looking for the most economical way to meet regulatory requirements.

To solve today's complex compliance challenge, firms need a solution that can record and capture data across all communication methods: Microsoft Teams and other IP connections, mobile devices, and fixed lines. Call recording should no longer be application-specific but needs to be unified across all networks, platforms, devices and locations.

By centralising both the recording and storage of conversations in one platform, organisations have compliant call recording from capture to storage. Not only are conversations compliantly recorded but, with voice AI, enterprises gain access to the data that can drive knowing the customer, accelerated investigations and remediation.

> **"The shift in enterprise focus towards building out more UCaaS capability drove interest in the potential of voice communications as a valuable source of data. There is a growing desire to understand conversational data and turn it into actionable insights through the use of AI. Businesses understand that voice data can be used to improve operational performance, especially with the increase of digital and distanced transactions."**
>
> *– James Slaney, COO*

Not all call recording is the same...

Recording on Microsoft Teams requires a more advanced solution that brings communications together.

Legacy Call Recording Vs. Unified Call Recording

Where legacy call recording solutions only offer a single end-point recording of voice calls, a Unified Call Recording solution reflects how modern workers operate in today's market environments. Workers often jump between Microsoft Teams across cloud and telephony connections (SIP), devices (mobile) and other audio and text-based communication channels.

Unified Call Recording can capture all audio recordings and conversations and store them in a single centralised system of record from multiple end-points.

15 compliant call recording imperatives for Microsoft Teams

With increasing regulatory scrutiny and workers communicating through multiple platforms, there is growing pressure on Compliance and IT Managers and senior leaders to ensure every conversation is not only recorded but accessible and auditable in real-time. Recording without the correct permissions, controls, storage and end-user management required for compliance puts organisations at significant risk. There are various security protocols that need to be in place to control access to recorded data and mitigate risk.

Here are 15 business-critical considerations to ensure that Microsoft Teams calls and conversations are captured and protected to satisfy regulatory mandates and improve investigations, monitoring, and surveillance procedures – whatever the communication channel.

1. Microsoft Teams-native Call Recording

Choosing a solution that directly integrates with Microsoft Teams and is certified by Microsoft Teams is paramount. Next, is ensuring the solution is cloud-based and and provides scalability, which is vital for teams and operations that involve a high volume of calls, such as trading desks and contact centres. The scalability provided by the cloud removes the restrictions of limited on-premise storage. Vast numbers of calls can be recorded concurrently and stored for extended periods in accordance with regulations.

2. Voice Intelligence Cloud

A Voice Intelligence Cloud, where voice data from recorded calls is transcribed and analysed by AI, provides a way for businesses operating in regulated industries to have a more proactive approach to compliance. The data extracted by the Voice Intelligence Cloud makes granular investigations more efficient; it also allows for real-time monitoring to aid compliance and surveillance teams.

> **"While Voice Data as a Service across mobile, UC, and SIP connections is a critical differentiator for service providers, the broader opportunity is in unifying that data in the Voice Intelligence Cloud and letting AI enrich it. This enables enterprises to turn compliant call recording into continuous compliance monitoring."**
>
> *– James Slaney, COO*

3. Encrypted, geographically redundant storage

Captured Microsoft Teams conversations need to be protected by encryption in transit with transport layer security and at rest. A cloud-native recording solution allows data to be stored in the capture region to ensure compliance with regional data sovereignty requirements. Regulations such as MiFID II can require companies to hold their recorded conversations for up to 7 years or even longer. Your compliance solution must have the storage capacity to store recorded conversations long-term securely.

Cloud storage has a significant advantage over on-premise storage, as data sets are protected with added geographic redundancy to meet data and privacy regulations. On-premise solutions can't compete with cloud platforms' ability to deploy across multiple data centres within a geographic region. Platform loads can be spread across data centres to provide full redundancy across all elements, including storage.

4. Cloud security

Storing conversational records securely is a vital component of regulatory compliance. With global operations common to modern business, firms will need to deploy a UCR solution that operates at a global level in order to ensure data sovereignty for each region they operate in.

For the purposes of (data) export for audit, access to recorded calls should be restricted to limited roles within a business, with strict authentication processes in place.

5. Critical metadata

Regulatory audits require a compliant data set to work off as a foundation. As part of these procedures and others – such as legal hold requests or dispute resolution – organisations are often required to retrieve all calls from a specific time or date.

Your recording solution should time-stamp all conversations and allow search results to be filtered by date or time and by user. Call metadata such as call participants, recording name, and any tags should be stored alongside a recording, in addition to any voice AI information.

6. PCI DSS considerations

Compliant call recording also needs to consider PCI DSS requirements. Some information can be stored and used, but sensitive information such as cardholder data cannot be recorded. Your call recording solution must have the ability to prevent the recording of this information: redaction is not enough. Choose a call recording solution with the right PCI compliance capabilities to meet the needs of your business.

7. Regulatory requests and trade reconstructions

Regulatory requests and investigations need to be responded to in a timely fashion. In industries such as financial services, firms may be required to provide full reconstructions of trades on demand, often with only 72 hours' notice, under regulations including MiFID II and Dodd-Frank. Real-time search and discovery make this easy – providing instant access to data to comply with audits or other requests for information. Choose a solution where all recorded calls are instantly available to search, replay, securely download, review, or delete on request.

8. Recorded voice announcements

Regulations such as GDPR and MiFID II require organisations to notify call participants that their conversation is being recorded. Optional recorded voice announcements (RVAs) automatically notify call participants at the start of an inbound or outbound call.

9. Proactive compliance through AI

Unifying recorded communications into one solution creates a repository of voice data that can be mined to improve regulatory compliance actively. By applying voice AI to recorded calls, the voice data can be transcribed to enable analysis and automate processes based on what was said during a conversation.

10. Retention periods

Deleting data once it's no longer required is as equally important as storing it securely in the first place. Particularly when it comes to compliance with regulations like the GDPR, organisations must erase data when they no longer have a legitimate purpose to store it.

Your solution should include the option to set retention periods for recordings so they are automatically deleted after a specified period.

11. Legal hold preparation

Legal hold requests can happen at any time. These events mandate the preservation of information, including recorded calls and texts, and can cause hassle for businesses if their data isn't stored in a unified repository. To cover legal hold requests, your solution needs to have a feature to preserve recorded conversation to prevent deletion under any circumstances. This should override standard retention periods, deleting a user, or the expiration of overall storage periods.

12. Proactively mitigating risk

Most industry regulations have been put in place to protect consumers and promote best practices. Your call recording solution can be a useful tool for proactive improvements and risk mitigation when it includes the power of voice-ai. When calls are transcribed, keyword alerts can be put in place for the early detection of risky behaviour or compliance breaches – deterring potential bad actors. When these words occur in a conversation, managers or supervisors will receive an alert with a link to the conversation in question.

13. Intuitive workflows and automation

Automation shouldn't stop at keyword alerts. To streamline processes within a business, your recording solution should include an open API that allows you to create intuitive workflows and rule-based automation. These can automatically populate other business applications for increased productivity and visibility across operations.

14. Identity provider-initiated single sign-on (IdP SSO)

Choosing a solution with IdP SSO makes granting and controlling access to recordings easy. Businesses can grant and manage access through their identity provider to ensure their specific security and access controls are adhered to when their users access recordings and sensitive data.

Businesses can selectively grant their users access to recordings using their existing SAML-compliant identity provider. User matching can occur either through a business email address or unique user ID, defined at configuration. Access controls can be boosted with password strength, validity period, (password) re-use restrictions, and any multi-factor authentication requirements managed within the business' identity provider.

15. Cryptography

Data should be fully encrypted by a recording solution, not only at rest but also in transit, using one of the strongest block ciphers available such as AES-256. Every protected object should be encrypted with a unique encryption key. This object key should then be encrypted with a regularly rotated master key, for added security.

Get started today!

Turn your businesses most crucial conversations into critical data that informs and empowers compliance success. Dubber captures conversations directly from the service provider network and UC platforms such as Microsoft Teams and aggregates that voice data into the Dubber Voice Intelligence Cloud.

> Need help transforming your businesses crucial conversations into meaningful voice data to achieve compliance outcomes, drive operational efficiency, improve service and sales performance, and reduce costs?

Contact us today for a consultation with one of our expert voice data solution specialists or visit **dubber.net** to learn more.

Get in touch ↗

North America

ATLANTA

3280 Peachtree Rd NE Floor 6,
Atlanta, GA 30305,
USA

DALLAS

1920 McKinney Ave,
Dallas, TX 75201,
USA

Australia

MELBOURNE

Level 5, 2 Russell Street,
Melbourne, 3000,
Australia

SYDNEY

5 Martin Place,
Sydney, 2000,
Australia

United Kingdom

LONDON

41 Corsham Street,
London, N1 6DR,
UK

dubber