telisca Recording White Paper

GDPR, MiFID II, PCI DSS

Reference: 190107

sales@telisca.com +33 1 46 45 05 12 www.telisca.com

1 GDPR in a nutshell

GDPR came into force on May 25th 2018.

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

The GDPR applies to every organization processing the data of EU citizens, regardless of where the organization itself is based.

1.1 What impact for call recording?

While the words "phone", "telephone", and "voice" do not appear in the text of the law, all personal data collected is subject to certain protections under the GDPR. As phone calls often include personal data such as names, addresses, health status, and other potentially sensitive information, the recordings must be protected in accordance with the law.

Companies wanting to record calls will need to give a good reason for doing so.

Several points to consider in getting your call recording strategy ready for GDPR include:- active consent, retention policies, the right to access to data, the right to erasure.

Also, the aim of GDPR is concern around data security, the protection of privacy, and the way companies process data.

1.2 Telisca Recording GDPR compliant

Article 7 : Conditions for consent Notify the customers that the call will be recorded, always ask for customer consent	Recording Notification is a telisca application that warns the user that the call will be recorded. It works for inbound, outbound and internal calls. Recording Notification is an option that can be added to telisca Recording.
Article 17: Right to erasure, right to be forgotten	You can choose the Selective or Automatic call recording, or which agents or lines to record. During the call, the customer could tell the agent his wish to not be recorded. Even in Automatic Recording mode, the agent can activate a button which informs the telisca server to disregard the current call.
Retention policy How long the recording is stored for depends on its purpose for storage.	Depending upon retention parameters, database search results will be filtered, excluding those results whose age exceeds the retention limit. In addition, a physical purge of the recording files is automatically performed. Different retention parameters can be defined depending of the company/department.
Article 25: Data protection by design and by default	telisca Recording support Secured SIP and Secure RTP Recording audios files are stored encrypted. Access to the web interface (https) to search and listen recordings is controlled by authentication based upon the

	CUCM user or an Active Directory login. Authorisation is segmented by company/department.
Article 30: Records of processing activities	History of recordings which have been reviewed (date, compliance officer, comments, …),

2 MiFID II in a nutshell

The 'Markets in Financial Instruments Directive' (MiFID II) came into force in January 2018.

Its primary goals were to foster harmonized function of financial markets, and enhance Investors protection.

From January 2018, all investment firms trading with or within the EU will be required to timestamp, report and store all communications relating to trading transactions for at least 5 years and, where requested by the competent authority, for a period of up to 7 years.

2.1 What impact for call recording?

- Record and store all communication.
- Quick access to records
- Maintain records for 5 years, at least. Store records securely

2.2 telisca Recording MiFID II compliance

Notify the customers that the call will be recorded	Recording Notification is a solution that warns the user that the call will be recorded, it is an option for the telisca recording solution
Retain records for all services, activities and transactions communications	All calls that lead to a transaction, even if orders were cancelled are recorded
Enable reconstruction of order activity upon request from client or regulator	Web interface to search recordings by META DATA Listen to streamed recordings via a web interface, with capability to download recording file
Retention policy at least 5 or 7 years	Archive recordings on efficient network storage or secure archive system. Forbid deleting the recording before purge delay. Handle purge management.

2.3 telisca Recording and other media

MiFID II stipulates that firms must take reasonable steps to record all relevant communications.

This includes all internal and external telephone conversations including SMS, Instant Messages and video calls across both fixed and mobile lines.

telisca Recording does not record desktop and Mobile conversations nor SMS.

3 PCI DSS in a nutshell

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

Every merchant accepting credit or debit card payments must comply with the Payment Card Industry Data Security Standard (PCI DSS), a set of twelve requirements mandating the protection of cardholder information.

Each of the twelve requirements focus on a different area of data security, ranging from how a merchant secures their network, to how they maintain a vulnerability management plan.

3.1 What impact for call recording?

PCI DSS sub-requirement 3.1 establishes a best practice of only storing the cardholder data that is absolutely necessary for your business.

So, try to avoid storing cardholder data during the call, whether by right or not within the call recording.

3.2 telisca Recording PCI DSS compliance

Notify the customers that the call will be recorded	Recording Notification is a solution that warns the user that the call will be recorded, it is an option available with telisca recording
During the call, Hashing the PAN*, the CVC** code, the expiry date, and the cardholder name.	telisca Recording offers a Finesse Gadget that allows the agent to pause the recording while asking the confidential information.
Strong cryptography	telisca Recording support Secured SIP and Secure RTP Audios files are encrypted. Access to the web interface (https) to search and listen recordings is controlled by authentication based upon the CUCM user or an Active Directory login.

*PAN stands for the Primary Account Number, or the 16-digit code found on every card
**CVC stands for Card Verification Code (or CVV, CVD), number is located on back of the credit card, except for American Express cards