TeleMessage

GDPR Compliance Deadline: May 2018

WHAT DOES IT MEAN FOR ARCHIVING?

In under six months, Europe's data protection regulations will undergo the biggest modernization in two decades.

The EU's General Data Protection Regulation (GDPR) is set to be enforced by 25 May 2018 - at which time non-compliant organizations will face heavy fines of up to 4% of their annual turnover. At present, Gartner predicts that by the end of 2018, more than **50% of companies affected by the GDPR** will not be in full compliance with its requirements.

WHAT IS GDPR?

The GDPR is Europe's new framework for data protection laws – it replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe.

The aim of this regulation is to protect EU citizen's data and privacy in an "increasingly data-driven world that is vastly different from the time in which the 1995 directive was established".

In effect, The GDPR directly affects the ability of organizations to make recordings of personal conversations, even those made on business devices.

KEY POINTS OF GDPR:

1. Increased Territorial Landscape

GDPR will carry an extended jurisdiction, as it applies to all companies and organizations processing the personal data of data subjects (customers) residing in the Union, regardless of the company's location.

The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU.

Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

2. Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the customers to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

The conditions for erasure include the data no longer being relevant to original purposes for processing, or a customer withdrawing consent.

3. Right to Access or Data Portability

The GDPR provides the customers the right to request and obtain information as to whether or not personal data concerning them are being processed, where and for what purpose.

Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

4. Consent

GDPR have strengthened the conditions for consent, and companies will no longer be able to use long illegible terms and conditions full of jargon.

The request for consent must be given in an intelligible and easily accessible form – using clear and plain language – with the purpose of data processing attached to that consent.

It must also be as easy to withdraw consent as it is to give it.

5. Breach Notification

Breach notification will become mandatory in all member states where a data breach is likely to 'result in a risk for the rights and freedoms of individuals'.

This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

GDPR and MiFID II: Conflicting Recordkeeping Requirements

Before GDPR comes into effect, another piece of Europe-wide regulation known as the Markets in Financial Instruments Directive (MiFID) II will become operative

On the surface, these two regulations appear to have conflicting objectives, with the enhanced monitoring requirements under MiFID II seemingly incompatible with the enhanced data protection requirements of GDPR.

As such, companies must consider how they will balance regulatory obligations under these two significant pieces of legislation to ensure compliance.

Under MiFID II, organizations are required to archive recordings of pertinent conversations that resulted or intended to close a trade, such as SMS, emails and voice call for five years.

On the other hand, GDPR requires excluding personal conversations, or when a consent was given, mandates that personal data should be kept in an identifiable format for no longer than necessary.

After that period, customers data should be securely wiped, or anonymized if organizations wish to retain

In the case of mobile recording, organizations may face a challenge in finding a viable way to record business calls without recording personal calls.

Even if the recording is never listened to, a firm is at risk of a breach of GDPR as personal calls could be classified as 'sensitive personal data'.

Considerations in Addressing Conflicting MiFID II and GDPR Recordkeeping Requirements

A key consideration when designing archiving procedures that are compliant with both pieces of legislation is whether records can be stored confidentially, ensuring only the business and those authorized within it can access these records.

Firms should also consider how to ensure the integrity of the records for the life of the retention period, ensuring they cannot be tampered with or deleted.

For firms using enterprise messaging solutions and call recording technologies to capture conversations relating to transactions, appropriate organizational and technical arrangements will need to be in place to distinguish these enterprise messages and calls from others where consent to record would be required under GDPR.

Archiving policies will also need to be regularly reviewed, not only for compliance with FCA expectations but also considered within the context of GDPR rules.

Companies will need to demonstrate how the proportionality, necessity, and data retention limitation principles have been taken into account when designing or extending recordkeeping policies.

Ultimately, it is important to note that GDPR and MiFID II regulations are not simply about recording conversations, but also to ensure that companies have a system in place for the regular reviewing and monitoring of such conversations on both company-provided and privately-owned devices.

TeleMessage is a global leader in enterprise mobile messaging solutions that offer robust and holistic mobile archiving platforms. Our Mobile Archiver is equipped with features that enable organizations to comply with archiving requirements such as: automatic deletion of records in case a customer decides to opt-out, data extraction and tagging, end-user notification in case of breach, and advanced data security options for maximum protection of customer data.

Visit our website today www.telemessage.com to learn how TeleMessage platforms can help you achieve compliance with the imminent GDPR implementation.

Created & Designed by: TeleMessage

Source:

http://www.eugdpr.org/key-changes.html
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
https://www.gartner.com/newsroom/id/3701917
https://www.telemessage.com/mifid-ii-almost-ready/