PwC & Solgari Industry Report

MiFID II & GDPR Compliance in the Cloud

pwc

Impact of MiFID II on Communications Data 3

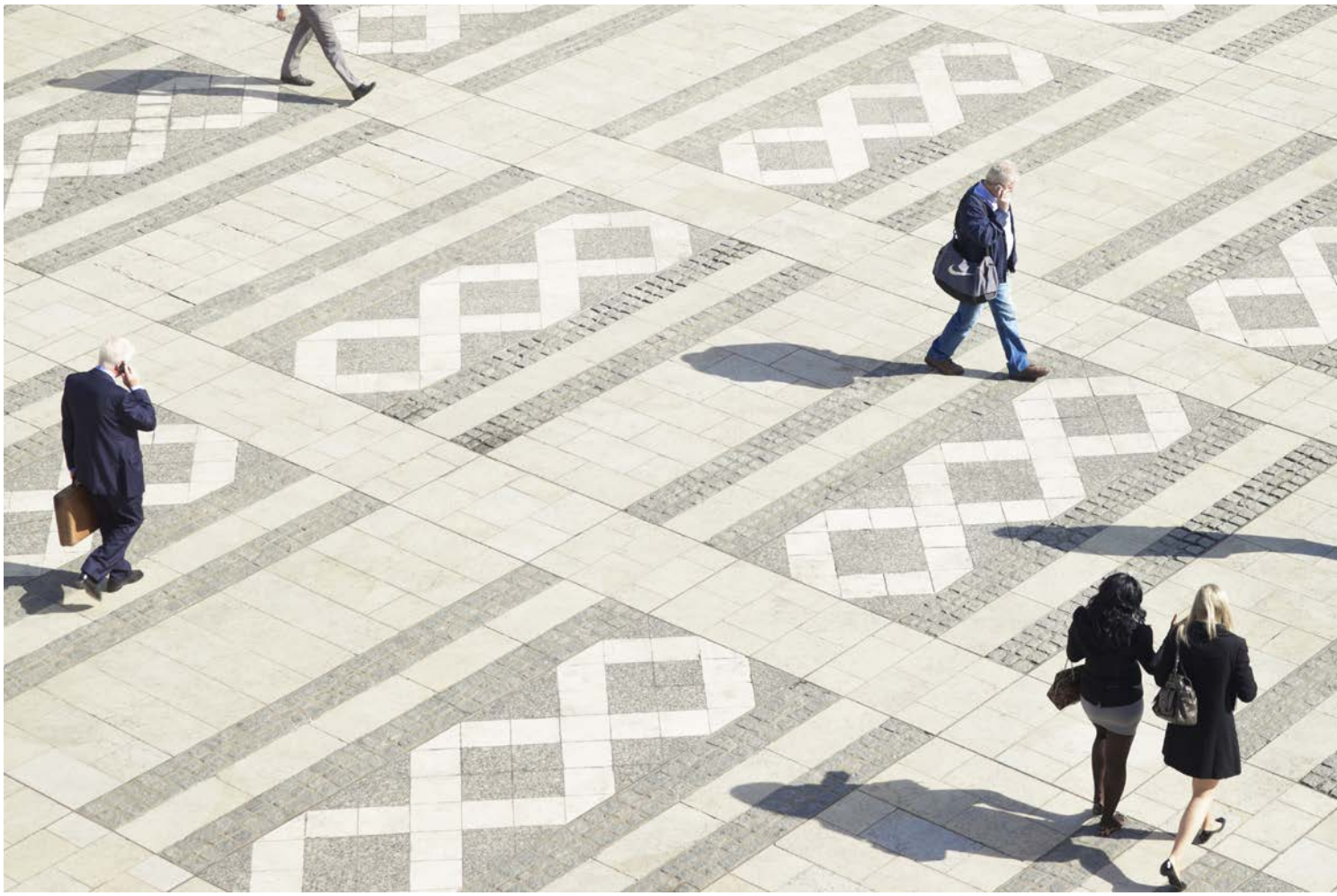
Impact of GDPR on Communications Data 4

Cloud Communication Software – MiFID II & GDPR Compliance within the Transaction 5

The four key layers of 'Compliance within the Transaction' 6

Final Thoughts 8

PwC Contacts 9



Impact of MiFID II on Communications Data

This year, 2018, marks the introduction of two hugely significant regulations in the form of MiFID II & GDPR. In this report, we assess the overlapping impact of these compliance requirements on communications data for Financial Services and FinTech firms and how integrated, omni-channel cloud communication software solutions not only address the demands, but also opens up significant big data opportunities.

Overview

Implemented in 2007, the Markets in Financial Instruments Directive (MiFID I) established a standard regulatory framework for financial investment service institutions across EU member states. Key to the directive's commitment to transparency was the requirement that firms record, retain, and make available for auditing all communications regarding "client orders and transactions". This increase in pre- and post-trade transparency requirements had a significant impact on investment and equity markets.

MiFID II is rocking the investment management industry, with the launch of an even more ambitious and extensive array of communications regulations, affecting a much wider range of financial firms than its predecessor.

Over the last decade, there has been a seismic shift in how investment and fund management firms communicate with clients, with mobile and fixed line calls now joined – if not replaced – by new technologies ranging from e-mail and SMS to messaging apps and video conferencing. MiFID II represents a concerted response by the European Parliament and Council to scale regulations to match the expansive variety of communications channels now used to engage with customers and prospects.

Introduced on January 3rd 2018, the directive will significantly enhance the robustness of financial markets by substantially increasing the level and scope of communications which need to be recorded and retained.

Under the regulations, any form of conversation or communication (even if no agreement or sale occurs) must be recorded for at least 5 years where it involves:

- The reception of an order/transaction from a client.
- The modification or cancellation of an order/transaction.
- The transmission of an order/transaction.
- The execution of orders on behalf of clients.
- The conclusion of an order/transaction.
- Any trades or affairs relating to an investment company's own accounts.

Although MiFID II is one of the most decisive directives ever to be imparted on the funds and investments industry, firms still lack understanding of its expectations and implications. Not only are there many grey areas in the directive, but transitioning to conformity is also perceived by many in the funds industry as a complex, expensive responsibility.

Ensuring compliance across multiple devices and platforms

The major issue for investment management firms under MiFID II is the extension of communications compliance. Whereas MiFID I related only to fixed calls, MiFID II extends to not only include softphones, desktop phones, and mobile phones but also "electronic communications", such as e-mail, online chat, SMS, messenger and third-party apps.

These newer platforms are critical to business success, given that customers now expect investment firms to offer video, text and other forms of real-time communications, not to mention the thriving bring-your-own-device (BYOD) culture and growth of remote working within the investment and funds sector.

Limiting or removing communications across multiple devices and platforms to prevent regulatory sanctions is not an option; investment management companies must instead find a way to bring their omni-channel communications in compliance with MiFID II.

The consequences of non-compliance

Companies found non-compliant with MiFID II will risk fines of up to €5 million, or 10% of global turnover with the reputational damage likely to be hard to repair.

Impact of GDPR on Communications Data

The introduction of General Data Protection Regulation ('GDPR') on May 25th 2018 represents a firm action by the European Parliament, the European Council and the European Commission to significantly strengthen and unify data protection for all individuals within the EU. While it should be heralded as a positive step, it is causing a frenzy as many businesses the world over are struggling to familiarise themselves with its potential impact. More worryingly, most are uncertain about how to even ensure compliance. However, this actually presents a unique opportunity for companies to transform their data protection procedures and strengthen public perception and customer confidence. There is also significant cross-over between GDPR and MiFID II allowing Financial Services and FinTech firms to equally invest in solving the compliance requirements.

The two main groups affected by GDPR

'Controllers'
Any organisations like ecommerce companies, financial institutions, recruitment agencies and pharmacies, who are responsible for recording customers' personal data such as economic, cultural or mental health information, and, for the first time, IP addresses, are known as controllers. Under GDPR, controllers must keep a record of how and when an individual gave consent to submission of their personal data. Controllers must also clarify how and why that data is processed, so that it can be deleted or moved if the owner requests it to be.

'Processors'
Any organisations like IT services firms, cloud services providers and payment solutions companies who are responsible for the actual processing of the data for a controller, are known as processors. Controllers will look to ensure their chosen processor abides by data protection law and maintain transparent records of their processing activities.

Crucially, if processors are involved in a data breach, they are far more liable for penalties under GDPR than they would have been under previous Data Protection Acts.

A European regulation, a global reach

Although created by the European Union, GDPR will have a global reach, governing the data of EU citizens all over the world. Even if controllers and processors are based outside the EU, the GDPR regulations will still apply to them once they are managing or processing data belonging to EU citizens. Once GDPR comes into effect in 2018, controllers must be able to immediately ensure that personal data is processed lawfully, transparently and for a specific purpose.

The consequences of non-compliance

The EU has promised significant fines for anyone found to be in direct non-compliance of the basic principles of GDPR. Where a company or organisation is found to have disregarded GDPR compliant procedures, they may be subject to fines of up to €20 million or 4% of their global annual turnover, whichever is the greater figure.

However, having GDPR processes in place is not enough. There are also large fines if procedures are followed but not quickly enough. Where a data processor discovers a breach, it is their responsibility to notify the controller, who in turn must contact the authorities and those parties affected by the breach. This all must happen within 72 hours. If this deadline is not met, companies and organisations may be fined up to €10 million, or 2% of their global annual turnover, whichever amount is greater.

These are both very serious potential consequences of not being able to demonstrate good data protection practices. Guilty companies are leaving themselves open to penalties that could significantly damage not just their financial stability but also their public reputation.

Cloud Communication Software – MiFID II & GDPR Compliance within the Transaction

Maintaining compliance across multiple investment market regulations

For investment management firms already struggling to maintain compliance with AIFMD, UCITS, EMIR, Dodd-Frank and MAR regulations – or preparing for the simultaneous arrival of GDPR in May 2018 - MiFID II presents yet another layer of complicated regulations to contend with.

In reviewing and implementing solutions and procedures to ensure MiFID II and GDPR compliance, investment management companies cannot afford to compromise on their ability to ensure continued compliance with existing or imminent legislation.

Engage with all clients on any channel through one cloud communications software platform

By transitioning to a compliant, integrated omni-channel cloud communications platform, an investment management firm can bring all communications channels together through a single cloud solution across all devices, allowing the organisation to engage with clients and prospects via voice call, video call, messenger apps, online chat and SMS.

Because communications channels and services are connected via secure user end points to the cloud communications platform and integrated with CRM systems such as Microsoft Dynamics 365 and Salesforce.com, all engagement can be easily recorded, archived, supervised and audited.

An instant solution requiring no capital investment

A switch to cloud communications does not require capital investment and provides instant resolution to MiFID II and GDPR compliance concerns, permitting the most cost-effective transition available. Firms do not have to risk losing customers by eliminating the use of certain communications channels, invest heavily in trying to bring legacy systems up to standard, or find themselves trying to tackle compliance channel by channel, using multiple solutions.

The four key layers of 'Compliance within the Transaction' delivered by integrated, omni-channel cloud communication solutions are set out below.

1. Discuss or create the transaction

Whether a financial services transaction is discussed or created using Voice, Video, Chat or SMS, an integrated omni-channel cloud communications solution with the appropriate security and compliance certification can deliver all this communiations capability on a per user per month SaaS model. This approach opens up automatic compliance and data analysis through having all the communication channels delivered through the same cloud service and is far more intelligent and efficient compared to the legacy alternative of using multipe vendors.

2. Record and archive the transaction

Regardless of the communication channels used to create the transaction, an integrated cloud communication software solution will record and archive the interaction for as long as required.

To satisfy GDPR, controllers will need to ensure military grade security and encryption of any customer data stored in call, video or data archives. Legacy telephony systems and most standard web collaboration systems do not have the capability to guarantee this level of security. However, cloud communication solutions, including PCI DSS compliant providers like Solgari, securely store and protect customer communications using 1024 bit military grade encryption in an ISO 27017 compliant hosting environment.

While regulatory compliance standards in the form of PCI DSS already exist with regards to protection of cardholder data, GDPR is likely to have an even greater impact. For starters, under GDPR, any breaches in relation to cardholder data will need to be made public knowledge. This places a greater than ever onus on controllers and processors to ensure the security of credit and debit card details.

3. Search and retrieve the transaction

MiFID II regulations demand that all data around the completion of transactions should be retrieved within 72 hours when required. If the communications have been recorded and archived using a compliant, integrated cloud communication software solution, search and retrieval should be instant. Companies can search across all channels, voice, video, SMS & chat to reconstruct any communications around the specific transaction.

4. Report and analyse the transaction

Once the relevant communications have been retrieved, significant reporting and search capability is available through cloud communication software solutions. As well as the communication reporting, it is also possible to word and phrase search within voice and video recordings to find specifics which may be required for dispute resolution, eDiscovery, micro or macro analysis. Unlike the traditional transcription solutions, using voice recognition technology such as Sondware from Solgari allows for far quicker and more accurate search of recordings. In addition, this approach is very effective in the context of GDPR as only the relevant part of a call can be extracted, leaving the rest of the data within the encrypted archiving environment. It also opens up tremendous big data opportunities to gain an overview of trends and views within the business and across customers and prospects.

Final Thoughts

MiFID II & GDPR represent significant challenges to the Financial Services industry, however many aspects of these new demands can be addressed by best of breed, highly secure cloud software solutions. Not only can these solutions lead to automated compliance, they are also likely to open up other opportunities around cost savings, efficiency and the ability to accurately access and assess very valuable data in the form of recorded communications.

Solgari Summary

Solgari provides Compliant & Integrated Omni-Channel Cloud Communication Services to FinTech, Financial Services, eCommerce, Retail, Logistics, Recruitment & Government customers in 33 countries to date.

Solgari's integrated cloud software service provides all the digital business communication channels – voice, video, chat & SMS – while automatically addressing GDPR, PCI DSS & MiFID II regulations through compliant recording & archiving of all communications.

Customers can access all business communications & related compliance requirements regardless of location on a per user per month SaaS model while avoiding the cost & complexity of legacy technology solutions.

Contacts

PwC
Birchstrasse 160
Postfach, 8050 Zürich

Dr. Günther Dobrauz
Partner
Leader PwC Legal Switzerland
+41 58 792 14 97
guenther.dobrauz@ch.pwc.com

Edward Grant
CFO Solgari
US +1-855-304-0022 x 302
UK +44 808 238 9584 x 302
IRE +353 1 246 1130 x 302
edward.grant@solgari.com

Michael Taschner
Senior Manager
PwC Legal Switzerland
+41 58 792 10 87
michael.taschner@ch.pwc.com

Orkan Sahin
Assistant Manager
PwC Legal Switzerland
+41 58 792 19 94
orkan.sahin@ch.pwc.com