MIFID2 and GDPR – When Opposites Attract

How to manage record-keeping under both regulatory regimes

Who this paper is for: Compliance, legal and IT decision makers that must tune and implement their organisations' response to the record-keeping requirements of MIFID2 and the privacy principles of the GDPR.

pwc

Introduction

The titans of new European Union regulation in 2018, MIFID2 and GDPR, – are invoking permanent changes in the way financial organisations must store their business records and manage customer data.

A key point of concern for financial intermediaries has been around two of the popular catchphrases surrounding the regulations:

- **From MIFID2 "Save everything about customers financial transactions for a minimum of five years"**
- **From GDPR "Individuals have the right to be forgotten"**

At the surface, these are two conflicting statements and regulations. However, upon closer inspection, both regulations can be managed and complied with by financial intermediaries. This article describes how organisations can achieve complementary compliance with both regulations.

Scope:

The GDPR is a vast topic and contains different applications to different industries and geographies.

This article is strictly focused on the record-keeping requirements of MIFID2 and the impacts of the GDPR to financial intermediaries that must comply with both.

Focus is provided on the lawful basis to process data into record-keeping systems, responsibilities of financial intermediaries to understand what personal data they have and their options to provide access and information to individuals.

The conflict

MIFID2 states that financial and business records surrounding transactions must be kept for a minimum of five years on a durable medium that cannot be altered or deleted.[1]

This data retention rule allows regulators to perform their mandates in the investor protection function of MIFID2. It is of extreme importance when the data they request from financial organisations is assured to be the unaltered data surrounding financial transactions. Why the focus on the original data?

- **Cybersecurity Risk** – In the current digital era, most financial intermediaries keep the primary data of their business in electronic form. It is not uncommon in the news to see outbreaks of data hijack, theft and alteration. What happens when a financial intermediary has had its data hijacked or altered? Can the regulator, business or customer truly respect data that may have been altered or damaged during a ransomware attack?
- **Information Risk** – Faulty IT systems, processes and controls play a role in the destruction, damage or loss of data. Without the necessary data in place, regulators and firms cannot perform their business and audit functions properly.
- **Fraud Risk** – Data falsification and editing are becoming greater problems as inside actors know how to manipulate information systems. They do so for their own purposes while obfuscating their actions in line of business information systems. When data is not saved to a repository that cannot be altered, the audit trail around a financial transaction may be obscured, thus preventing organisations from ever knowing what truly happened during an incident. This in turn impedes regulatory and judicial investigation.

As required by MIFID2, a true copy of the data in a fully audited record-keeping system helps protect against the three issues above. Regulators are required to understand these challenges – from both the customer and the financial organisation's perspective.

The GDPR provides an ecosystem of fundamental data subject rights and the one that most conflicts with MIFID2 at the surface is the Right to Erasure (Article 17). This data subject right appears to contradict MIFID2's requirements for the preservation of data. Upon further inspection of the GDPR, it is clear from its data processing articles[2] that financial intermediaries gain the lawful right to preserve data under the basis of Legal Obligation.

Individuals that are not well versed in the technicalities of the GDPR may see the right to erasure as an absolute right or one in the context of non-financial services and call upon this right creating an unnecessary burden for financial intermediaries and their regulators. One of the most important tasks of the financial industry is to get in front of this by making it clear to customers what their rights really are in a clear and transparent manner – which by the way is a mandate of the GDPR by way of privacy policies.

To help readers gain insight for their policies and actions under the GDPR with respect to MIFID2, this white paper discusses the lawful reasons for processing, how they affect data subject rights and best practices when archiving records.

Lawful Basis for Record-Keeping

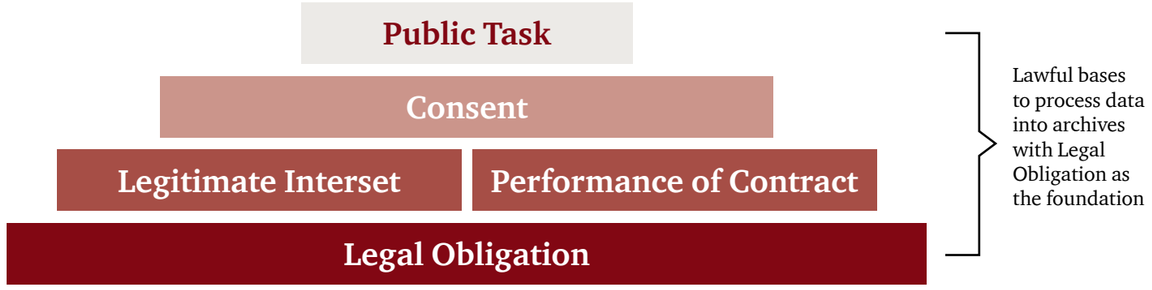
GDPR provides six reasons for the legal collection and processing of personal data[3]:

- **Consent**
- **Contract**
- **Legal Obligation**
- **Vital Interests**
- **Public Task**
- **Legitimate Interests**

The lawful basis most relevant to MIFID2 record-keeping is the Legal Obligation. What data processing rights does this Legal Obligation give regarding MIFID2?

It allows financial intermediaries to execute transactions on behalf of individuals in a personal or fiduciary capacity using content reflective of the current digital era. For the proper allocation of financial products to their owners, this content most likely will contain personally identifiable data. The end state of content that generates financial transactions is the archiving of the content containing personal data into semi-permanent[4] archiving systems – aka "record-keeping".

Data records have to be preserved for a specified retention period to ensure that regulators, companies and customers have access to key business records surrounding financial transactions. In the interest of regulating and harmonising national and EU-wide finance, financial and business records must be kept to allow proper investigation of financial transactions by organisations and their regulators. While MIFID2 states that data has to be kept, GDPR highlights the right to be forgotten. To comply with both regulations financial institutions have to monitor various legislations on the required retention periods and amend their deletion processes for electronic and physical archive systems correspondingly.



1 MIFID2 Final Report, December 19, 2014 (ESMA Technical Advice), Section 2.6, Storage & MIFID2 Delegated Regulation Article 76(10)
2 GDPR Article (6)(c)
3 GDPR Article (6)(c)
4 A "semi-permanent" archive is one that holds data for a limited time such that the electronic data cannot be altered or deleted until an expiration date when the data becomes available for alteration or deletion. This type of electronic system is often identified by the technical term "WORM" storage (Write Once Read Many).

What kind of personal data would be processed into record-keeping systems?

The following table outlines the most significant content record sources used by financial intermediaries to execute their contracted responsibilities. This list is not exhaustive and will vary depending on the products and sales strategies of financial organisations but is a good starting guide to what is at stake.

Note that MIFID2 is an EU directive, not a national law. However, the directive requires that all European Union nations transpose MIFID2 into national law. From a technical perspective, records kept under MIFID2 are kept as per the nationally transcribed legislation of the EU member state. The term "MIFID2 record-keeping" is an umbrella term to describe the source of the national law. It is advisable that when drafting GDPR documentation, financial intermediaries cite both the nationally transcribed law and MIFID2 as the lawful bases for record-keeping.

It is advisable that financial intermediaries inform their customers of their lawful basis for record-keeping, whether they do it on premise or by cloud service partners. If a third party cloud partner is involved, they are considered a data processor and documentation should be established between the financial and the third party that outlines the permission they have given to the third party to process data and the lawful reasons to do so. This should be done by establishing a data transfer agreement with the third party that processes the data.

Content record type	Personal data in content metadata	Personal data in content
E-mail	E-mail addresses, display names, possibly IP addresses in routing information	Text/media in the subject and message body that identify an individual.
Instant messaging	"Chat names", display names, chat system IDs.	Text/media in the message body that identify an individual.
Phone call recordings	Phone numbers, extensions, display names	Audio media that identify an individual by spoken word. If transcribed, then in text.
Documents (contracts, statements, notes, etc.)	Content creator names or identifiers (ex.: LEIs), fiduciary and chain of custody identifiers	Text in the document body that identifies an individual.
Transactional content (market orders, contracts, etc.)	Content creator names or identifiers (ex.: LEIs), fiduciary and chain of custody identifiers	Text that identifies an individual in the body of the contract or order.
Line of business system reports	Content creator names or identifiers (ex.: LEIs), fiduciary and chain of custody identifiers	Text that identifies an individual in the report.
Photographs, videos, biometrics (may often be attached to other content types)	Content creator names and personal identifiers if visual and biometric tagging are done	Visual media that contain images of an individual or their biometric information.

Lawful bases can be thought of as building blocks as shown in the diagram on the previous page. As just described, the foundation of lawful basis to process data in record-keeping systems for the financial industry is that of legal obligation. Based on the services and functions provided, financial intermediaries may choose to add additional lawful reasons for the processing of personal data in record-keeping systems – and some may be necessary once the end of the minimum retention periods of MIFID2 approaches in January of 2023. The following table outlines secondary and possibly tertiary lawful reasons to process.

Secondary Lawful Reasons for Record-Keeping

Lawful basis GDPR Article Reference	**Application to financial organisations**	**Personal data in content**
Consent Article (6)(1)(a)	In the scope of financial transactions, consent is intrinsically connected to Performance of Contract. This topic is separate from consent for marketing purposes which is not covered in this article. Customers cannot opt-out of record-keeping when an organisation has a legal obligation to keep records. However, it is best practice to inform customers that their records will be kept in an archive under the scope of EU and national laws.	Customer receives a special discounted interest rate offer by email after explicitly consenting to targeted marketing, reviews it, and proceeds to apply for the special interest loan via a connecting URL to a website hosted by the financial. As a solicitation for a special rate, the customer's personal data was used to communicate to the customer. An email with personal data is now archived in the financial intermediary's record-keeping system as the source communication in a commercial solicitation that led to a financial transaction.
Performance of Contract Article (6)(1)(b)	Contracts with customers that lead to financial transactions are business records under MIFID2 and will require record-keeping. Executing the contracts properly constitutes lawful basis for processing of personal data. Under most contract law, parties subject to the contract must be identifiable. For a financial intermediary, the identification of parties to contracts is key to the performance of the contract as ownership of funds and securities is of primary importance. Personal data will be in the contracts as a means of identifying the parties. In a consumer contract, identifying personal data of the individual will be enclosed. In a business to business contract, the personal data of custodians with authorisation to act on behalf of the business will be in the contract.	**Business to Consumer:** A customer signs a loan agreement that allows the financial institution to process their personal data such that funds are transmitted to an account that the customer owns or is a legal custodian. **Business to Business** (example one)**:** A corporate customer has a fiduciary custodian of its accounts (typically, a treasury department staff). Said custodian requests transfers of funds between business accounts. Personal data is used to identify the custodian and record their authorisation to move funds. **Business to Business** (example two)**:** A corporate or non-profit customer with a securities account at a brokerage instructs the brokerage to conduct market buy or sell orders. Personal data of the individual making the request is used to record authorisation to trade and to properly clear and attach ownership to the securities that are subsequently processed.
Vital Interests Article (6)(1)(d)	This lawful basis is typically used when data needs processing to protect a life. (This lawful basis is not a key component for financial intermediaries, more so for healthcare.)	N/A
Public Task Article (6)(1)(e)	It can be argued that when a financial or consumer are under regulatory, civil or criminal investigation, preservation of financial records is a Public Task as the justice system requires records for investigation. The public interest is at stake when illegal and unauthorised financial transactions have been conducted and records must be acquired for investigation.	Under MIFID2, records must be kept a minimum of five years. At the expiration of the five years, financial intermediaries must make decisions as to whether the data should be deleted or not. If there are legal holds on the data from the courts, then there is a lawful basis to keep the records with personal data as a function of the Public Task necessary to complete a judicial process.
Legitimate Interests Article (6)(1)(f)	Under strict regulation, financial intermediaries need to execute their responsibilities otherwise, they themselves become targets of regulatory and judicial actions. While the law says they must keep certain records for a minimum time span, they still can choose to do so above and beyond what the law sets as a minimum for their own protection – and possibly that of their customers. Financial intermediaries must be prepared to document, explain and defend their legitimate interests if this is chosen.	**Examples:** If financial data expiring in 2023 five years after the implementation of MIFID2 is not under legal hold, and customer data no longer must be kept in semi-permanent storage, a financial may decide that the data should remain in the archive while the customer is still in fact a customer. Another example is if the customer has stopped doing business with a client, then the company may decide to keep the archived data records up to an additional number of years to ensure they have account records up to the end date of a statute of limitations that may allow the former customer to sue the financial. The archive extension time frames would vary across different nations.

Rights and Record-Keeping

With the reasons for the lawful processing of data into semi-permanent archiving systems established, let's look at the rights of individuals granted by the GDPR with respect to MIFID2 and financial record-keeping.

At the onset of the GDPR, individuals may not immediately understand that their popular rights granted by the GDPR are not absolute. Especially when financial intermediaries are under Legal Obligations to process, they may not be able to exercise all their rights.

GDPR listed rights GDPR reference	MIFID2 record-keeping application
Right to access (Article 15)	From a regulatory perspective, this right is available from both MIFID2 (Article 16(7)) and the GDPR. ESMA, the pan-EU financial regulator, has in fact commented on the idea that companies are required to provide financial data about their customers when requested and without excessive delay.[5] MIFID2's statement regarding client access to records is specific to electronic communications and voice recordings archived in the context of financial transactions. GDPR expands this scope to include all content that may contain an individual's personal data. Each financial intermediary will have its own IT systems and archiving ecosystem. If records from line of business systems are duplicated in record-keeping systems, there should be a clear audit of the archival process. This may allow firms to only provide copies and information about personal data from the original source system. However, they would still need to inform data subjects that the same records are in the archival system. There are also use cases where firms may choose to export from only the archive system. For instance, some data may have been moved to off-line archival storage for application performance purposes with the firms knowing a copy is preserved for record-keeping compliance.
Right to rectification (Article 16)	For data in MIFID2 electronic archives, this will not be possible. By regulation, the data will be in a format that cannot be altered or deleted ("WORM"). For content in line of business systems, this could be possible within the framework provided by the GDPR but treated outside of the scope of record-keeping.
Right to erasure (Article 17)	For MIFID2 record-keeping purposes, information stored in semi-permanent archives ("WORM") that are designed to not be altered or deleted cannot be deleted. The reasons are explained in the previous section. Individuals will have the right to request erasure but financial intermediaries will be able to refuse the request from semi-permanent archives due to regulatory edict. To deal with incoming requests it is suggested to have clear processes in place, be aware of all data storages and to consider the regulatory retention periods.
Right to restrict processing (Article 18)	This right will be hard to contest by individuals. Nevertheless they can obtain that processing of the data is restricted if erasure is not an option. The GDPR makes it clear that financial intermediaries can use their Legal Obligation under MIFID2 and national laws as the lawful basis for the archiving of records into semi-permanent archives. Financial intermediaries should continue to store electronic records as they are mandated as only extraordinary circumstances would have judicial and regulatory authorities stop financial record-keeping as mandated by EU and national law.
Right to data portability (Article 20)	This right is one that may or may not have much impact on record-keeping depending on a financial intermediary's overall record-keeping programme and technical capabilities. If a financial intermediary has acquired the means to do efficient data export and sharing, it would be done from active data in line of business systems. It would be rare for the business to export data from the archival system – unless: • It involves content that may have already been purged or deleted from line of business systems for any number of technology reasons. • The firm feels a significant performance impact on production systems may occur, thus making export from archiving systems more desirable. (In fact, this may be an unforeseen value add to the record-keeping system for consumer facing financial intermediaries that decide to honour data portability requests.) The management of data export will be contingent on the system and process needs specific to the organisation. In general, best practice would be to ensure that the export of content that must be exported is done in a consistent and auditable manner with low IT systems impact. While a specific form of the data extract is not required, GDPR states that the extract needs to be readable by a machine and forwarded to a new processor if requested by the client.
Right to not be subject to decisions based on automatic processing (Article 22)	Monitoring of financial transactions is mandated under two sets of recent financial regulation: • MIFID2 states that compliance must periodically monitor financial transactions for accuracy, lawfulness and confirmation that proper records are in fact stored.[6] Given the task of monitoring communications for hints of financial non-compliance, some firms are using new FinTech/RegTech solutions that attempt to automate the flagging of negative activity given the large amount of data produced by many financial intermediaries. Typically, BigData systems with Artificial Intelligence (AI) analyse key words, numerics, and statistical activity to flag content that may violate regulatory policy. Ultimately, individuals are behind the analysed content and they may be targeted for additional supervision or flagged for non-compliance. Under the GDPR, this could be considered as affecting the individual in a legal or significant way. • Firms involved in the securities trading markets must undergo "T+1" market transaction surveillance. This is used to detect fraudulent trading activity. Much of the content flagging in these systems is automatic and can also lead to the flagging of individuals (traders, investors) in a legal or significant way. GDPR Article (22)(2)(b) does provide cover for financial intermediaries to do this type of monitoring as it is authorised under EU and national law – once again, MIFID2 and its national counterparts.

5 ESMA Questions and Answers On MiFID II and MiFIR investor protection and intermediaries topics, May 25, 2018, page 39 as footnote 17 and Question 9, page 42. ESMA document: ESMA35-43-439.

6 MIFID2 Article 16(7) and Article 76 of the MIFID2 Delegated Regulation

Data Masking

Data masking is a technical response to the GDPR that helps organisations fulfil some of their data protection accountability requirements. The two most commonly used methods are stated below:

- Pseudonymisation – The process of replacing personal data with an artificial identifier that cannot be used to identify an individual by appearance. A link to the original personal data is maintained elsewhere. This method allows for the reconnecting of an individual to a data record. Legal entity identifiers used in transaction reporting are a good example of pseudonymisation. Pseudonyms are still considered personal data as an individual can be identified when the data are linked.

  For financial intermediaries that use this method with line of business applications for any applicable reason, the original content records will need to be archived with the pseudonyms intact and importantly; they must also archive the mappings that can be used to reconstruct the identity of the individuals that were masked. The reason for this pragmatic approach is that MIFID2 has strict standards for the identification of parties in financial transactions for the obvious reasons of the prevention of money laundering and other financial crimes.

- Anonymisation – The process of completely changing the data that may personally identify an individual such that the content can never be used to identify an individual again.

  It is most likely not a good idea for financial organisations to anonymise content surrounding financial transactions as they and their regulator may not have a viable mechanism to reconstruct and investigate financial transactions.

  Anonymisation could be used in secondary situations such as the usage of BigData, AI and Data Warehouses to analyse financial transactions for metalevel insights. It would not be necessary for the data technicians performing these types of analyses to know the exact identity of individuals. If the data were being used to target individuals for marketing purposes, then there could be issues that financial intermediaries may have to further mask or obfuscate the transaction so that technicians do not have access to financial data about specific individuals.

Of the two processes, anonymisation creates more hurdles for financial intermediaries to consider. What is clear however is that content surrounding financial transactions can be pseudonymised for record-keeping but not anonymised data.

Best Practices for Record-Keeping

This article assumes that financial intermediaries acting in the data controller role have created privacy plans for their customers outlining the processing, cybersecurity protection and transfer of their data to subprocessors.

If not done already, it is recommended that they also specify the reasons for record-keeping as records in semi-permanent storage may become problematic if their customers are not aware of the reasons they are kept. The following sections provide further best practices specific to the record-keeping process. The recommendations are in addition to what financial intermediaries may have already documented around processing, data protection and cybersecurity of personal data.

Data Protection Statements

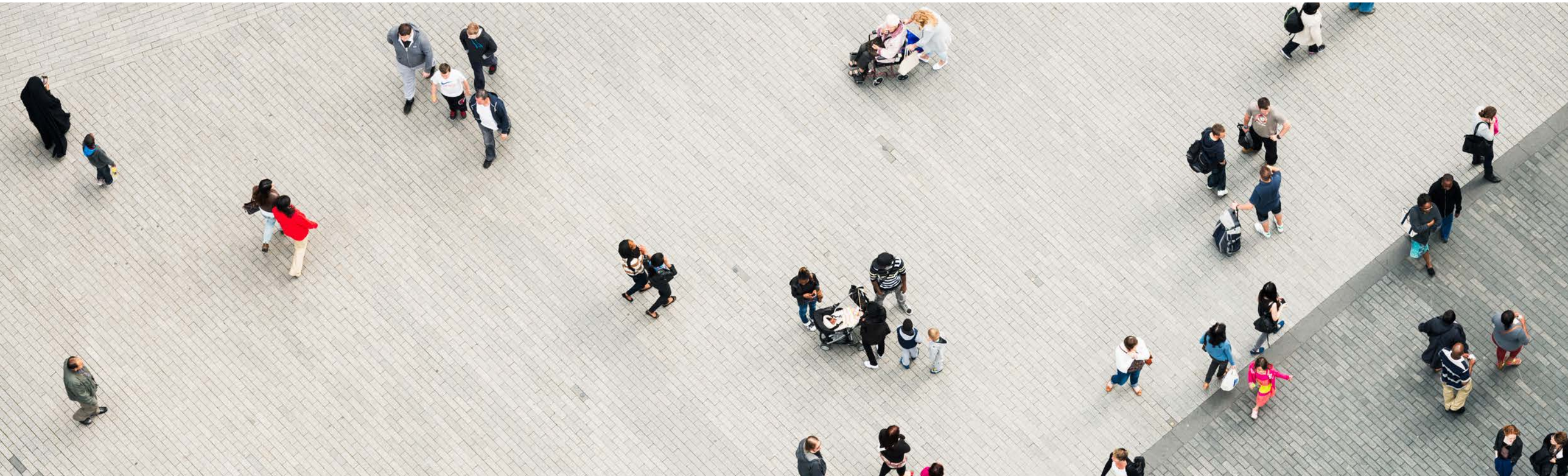
- Specifically mention why data in semi-permanent storage is kept for the timeline mandated by the national regulator under MIFID2.
- Outline which rights the organisation will grant individuals concerning content that contains their personal data.
- Specify the limitations to the rights the individuals can have on the semi-permanent records.

The Record-Keeping Process

- If possible, attempt to centralise as much archiving into a single compliance repository. This will make managing personal data in the archives much easier versus doing it across multiple systems from multiple vendors.
- Determine the regulatory content that must be archived and what personal data it may contain.
- In the archiving system used, ensure there are ways to tag or classify content that may contain personal data and the lawful basis for their processing.
- Ensure there are catalogues of personal data. Typically, these would be identity management systems within content generating applications. Master data management or centralised identity management systems would work even better.
- If possible, identify personal data in content that is being collected by archiving systems and tag it within content indexes. Catalogues of personal data would facilitate this more efficiently.

Data Masking

- If data masking is used for regulated content, ensure it is archived in its original form and that the catalogue to translate identities is also archived.
- Unless necessary, do not archive anonymised data into regulatory record-keeping systems. It serves no purpose from a regulatory archive perspective. Do back it up for IT purposes.



Data Portability and Export

- If providing data for export from right to access or data portability requests, determine which systems will be used to export located data. This could be the original business system or it could be the record-keeping system, or a combination of both.

- Ensure that there is an auditing system that keeps a history of requests and the personnel that submitted and conducted the requests.

- Ensure the data exports contain information about:

  a. The lawful basis to process and keep in semi-permanent storage. Typically, MIFID2.

  b. The source of the data. The name of the system that generated the content. For example: corporate email system.

  c. The date the content was generated and archived. Ex.: January 3, 2018.

  d. The categories of content. Ex.: email, faxes, customer statements, voice call recordings.

  e. The categories of personal data found. Ex.: email addresses, full names, phone numbers.

  f. The presence of pseudonymous data. Ex.: legal entity identifiers would need to be pointed out.

  g. The retention period of the data. Ex.: the data is in the semi-permanent storage system for a minimum of five years.

  h. If necessary, whether the data was used for automated decision making.

  i. If necessary, whether data was transferred to third countries.

- Much of the discussion about individuals has so far revolved around customers of financial intermediaries. Employees also have rights under the GDPR. If exports would expose employee personal data, they must in turn be advised that such events could happen. This would normally be part of an employee rights policy document. An example would be that emails between a customer and a financial would have the email address of the employee. This is in the normal course of business and is expected, but management of employee rights is also important and required.

Choice of Record-Keeping Systems

Given the unusual timing that MIFID2 and the GDPR are going into effect the same year, EU-based financial intermediaries are in a unique position to make IT decisions about their record-keeping that could enable better compliance with both regulations.

- Firms should develop a strategic record-keeping programme for their MIFID2 compliance. The reasons and details for such a programme are outlined in the following PwC and KSF Technologies article: **https://news.pwc.ch/34673/mifid2-ready-new-era-record-keeping/**

- The systems should have strong identity management features internally or the ability to connect to external systems. This will be important for the gathering of personal data for content tagging.

- The systems should have robust content tagging and classification features so that personal data can easily be found from the archives. This also creates the ability to get system-wide personal data summary reports on a per content type basis.

- The systems should be able to apply data governance metadata to content to ensure that data lineage is tracked should data be distributed via APIs or archive exports. This helps track the movement of content with personal data from one information system to another. Knowledge of where data is transported is of key importance in the GDPR.

- Besides the ability to provide legal exports with clear audit trails and data verification, the system should also be able to provide GDPR exports that provide data required in exports from right to access requests as previously outlined.

- Solutions such as the Arkivy Record Keeping Operations System produced by KSF Technologies; the co-authors of the paper cited provide these types of functionality.

Personal E-Discovery

E-Discovery is short for “electronic discovery.” This is a semi-legal term used to describe the legal process where data and documents are sought by lawyers and the courts for judicial proceedings.

Given the scope of the right to access and data portability under the GDPR, all firms that must be compliant with the regulation will see a vast boom in their requirements to offer “e-discovery like services” to their data subjects. As regular targets of consumer and investors, financial intermediaries must especially prepare themselves for the operational complexities of this task.

The Hidden MIFID2 Regulatory Danger of the GDPR

With greater numbers of individuals asking financial intermediaries for the records that concern them due to the personal e-discovery boom mentioned above and with privacy documents in hand that contain information about records also being kept in semi-permanent financial archives, firms may find themselves in a situation that when financial records are produced from archive system specific right of access exports, they may not be complete or unavailable if the firm’s record-keeping has had gaps in its archiving of regulated content.

This is a situation that may trigger data subjects to register complaints with their data protection regulator which may also lead to a complaint with the financial regulator – who in turn may be very curious to know why records are not available in the MIFID2 archives. By its nature of allowing greater surface area for individuals to request content from financial intermediaries, the GDPR may paradoxically increase the risk of detection of financial intermediaries that are not compliant with their MIFID2 record-keeping. Since ESMA has stated that customers have the right to request data under both MIFID2 and the GDPR, refusals to provide content to individuals due to faults in record-keeping will not be so easy to overlook by the regulators.

Conclusion

Financial intermediaries have a duty under MIFID2 to keep the records of their financial transactions. It is a legal obligation that comes from European Union and national law. The GDPR can guide the protection of data in the systems used to archive financial data, so it harmonises well with MIFID2 as the protection of data in archives is a benefit to financial intermediaries, their customers and the regulators. The GDPR with its exceptions for the processing of data due to legal obligations does not conflict with MIFID2 when analysed in detail. Both MIFID2 and the GDPR provide opportunity for individuals to exercise their rights within the limits of the regulations while still ensuring data are archived properly to ensure a functioning financial system.

Though financial intermediaries may dislike it, MIFID2 has made it mandatory for them to keep a live and archived copy of their regulated content. The GDPR makes them manage the data in both repositories in the same manner, thus replicating data protection practices and further increasing their regulatory burden. With the GDPR, financial intermediaries will have more incentive to get their record-keeping right as it also increases the possibility that a failure in record-keeping will be detected due to the increased frequency of data subject requests and their rights to seek regulatory action if not satisfied that all data have been provisioned.

With a strategic record-keeping programme and an archiving system that is GDPR ready, financial intermediaries can be compliant with both regulations in a more efficient manner from the collection of records to the export process driven by right of access and data portability requests. If a strategic record-keeping programme is engineered well enough and content archived into a single compliance repository, it may be that all right of access and data portability requests can be executed from the record-keeping system, thus shifting the burden from multiple line of business systems and giving MIFID2 and GDPR enabled record-keeping systems added value for financial intermediaries.

Contacts

PwC
Birchstrasse 160
Postfach, 8050 Zürich

Günther Dobrauz
Partner & Leader, PwC Legal Switzerland
guenther.dobrauz@ch.pwc.com

Michael Taschner
Senior Manager, PwC Legal Switzerland
michael.taschner@ch.pwc.com

Philipp Rosenauer
Manager, PwC Legal Switzerland
philipp.rosenauer@ch.pwc.com

Orkan Sahin
Assistant Manager, PwC Legal Switzerland
orkan.sahin@ch.pwc.com

Contacts: KSF Global Services, LLC

KSF Global Services LLC
Bahnhofstrasse 52
CH-8001 Zürich
Switzerland
Tel: +41 44 214 62 88
Fax: +41 44 214 65 19
Email: info@ksfglobalservices.com

Michael Imfeld
Managing Partner Business Development
michael.imfeld@ksfglobalservices.com

Allen Frasier
Director of Compliance Applications
allen.frasier@ksfglobalservices.com