shield.

GDPR & Compliance:
What you need to know

HANDBOOK

Table of contents

Introduction

The General Data Protection Regulation (GDPR) was a landmark moment in the evolution of data privacy law, and since ratification it has served as the baseline for similar global legislation.

In July 2023, the European Commission proposed a hardening of enforcement of the regulation with additional rules related to cross-border data protection probes. By refocusing efforts into oversight and investigations, the European Union has bolstered GDPR and added more fangs to a regulation that already triggers uncertainty, worry and confusion for compliance teams.

Five years after its final implementation date, with multi-million and billion-dollar fines issued to firms who were in violation of the law, achieving GDPR compliance has never been more crucial.

For financial services firms, GDPR's intersection with other regulations and standards has created a tapestry of requirements to navigate in order to stay compliant.

One of the most critical considerations is how GDPR overlaps with communications surveillance and eDiscovery, putting a premium on the ability to ensure data security and regulatory adherence when investigations take place. How firms handle the personal information and communications of staff has become paramount to regulators viewing fidelity to compliance through a GDPR lens.

GDPR in context

NICE TO KNOW

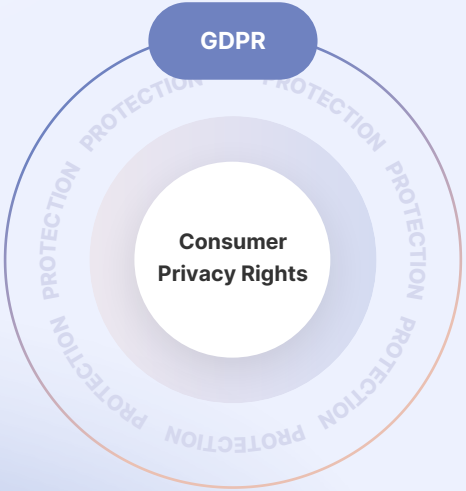
PII:
'Personal data' shall mean any information relating to an identified or identifiable natural person ('Data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference in particular to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (GDPR, Article 4).

NICE TO KNOW

Data Protection Officer:
A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing a company's **data protection** strategy and its implementation to ensure compliance with GDPR requirements.

GDPR enters the enforcement era

There can be little doubt that GDPR has been a success in how consumer privacy rights have been protected, with clear guardrails for how businesses should handle data that passes through the EU. Post-Covid, however, global supply chains, disparate workforces and international corporate presences require data to be shared across borders in unprecedented volumes.



Questions have been raised on the data transfers required for banks in particular to comply with international regulations around anti-money laundering (AML) and sanctions. It is still the case that many organizations, particularly those outside of the EU, still struggle to comply, and there is no one definitive way for businesses to achieve full compliance.

Fines were not particularly large in the early years, but that changed in May 2023 when Meta, the parent of Facebook, **was fined $1.3bn** and given a 6-month window to stop data transfers from the EU to the US. The decision notice stated that while Meta had policies in place to treat EU data differently from a legal standpoint, it couldn't demonstrably show it could do so.

“This ruling puts an end to paying lip-service to compliance,” said Jedidiah Bracy, of the International Association of Privacy Professionals.

“Without demonstrable controls governing data movement, a company will find itself outside the law and therefore liable.”

Meta’s fine removed any lingering doubts that data protection, and proof of data protection, is a necessity rather than an optional policy, and one every business must adhere to.

Data protection policy → **Optional** **Mandatory**

The severity of the punishment makes a strong case for broader automated data classification tools across businesses, particularly in the surveillance function. These tools are able to categorize sensitive data as identified in the business environment based on the appropriate compliance regulations, level of sensitivity and other custom criteria, such as the company’s data retention policy.

From here, data can be securely processed and used by authorized individuals within an organization, and eventually, disposed of in accordance with its retention policy.

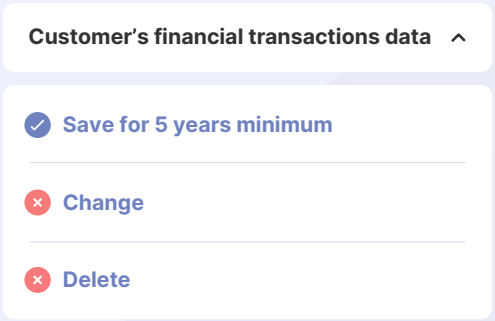
Regulatory risks and challenges

GDPR, recordkeeping and the MiFID II problem

Non-existent or poor recordkeeping practices are one of the main stumbling blocks to GDPR compliance. Low-cost electronic storage, databases and search tools have significantly impacted records classification and life-cycle management, and often mean personal data is never consistently erased. Over-retention of data is common, and the 'right of erasure', one of the most notable articles of GDPR (17), has proven a significant obstacle for many financial services firms.

It can also have the knock-on effect of undermining another GDPR requirement, the Register of Processing Operations (Article 30 aka ROPA), which requires, among other attributes, a name and purpose for each processing operation that uses personal data, and a time-limit for storing this information.
The right of erasure, also known as the 'right to be forgotten', appears to directly contradict the demands of a key piece of financial services legislation which concerns every aspect of a bank's operations; the second Markets in Financial Instruments Directive (MiFID II).

Under MiFID II, all data surrounding a customer's financial transactions must be saved for a minimum of 5 years, and that data cannot be altered or deleted. It also requires firms to collect and retain records of all communication with customers, including phone conversations and digital communications. The rules exist to help regulators perform checks and investigations to uphold investor protection standards and protect the integrity of financial markets, making unaltered data surrounding transactions a primary concern.



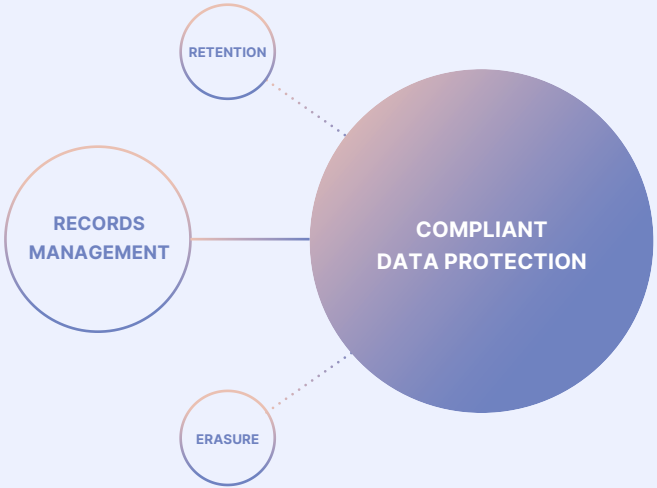
Regulators have to be certain they are reading the original data to guard against alterations following cyberhacks, IT glitches, and fraud risk, a requirement which ostensibly clashes with GDPR's stance. There are carve-outs in GDPR, however, with 6 lawful reasons for firms to preserve data, one of which being 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," said Günther Dobrauz, partner and GDPR expert at PwC Legal Switzerland.

"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 comply with both regulations, financial institutions have to monitor various legislations on the required retention periods and update their deletion processes for electronic and physical archive systems correspondingly.

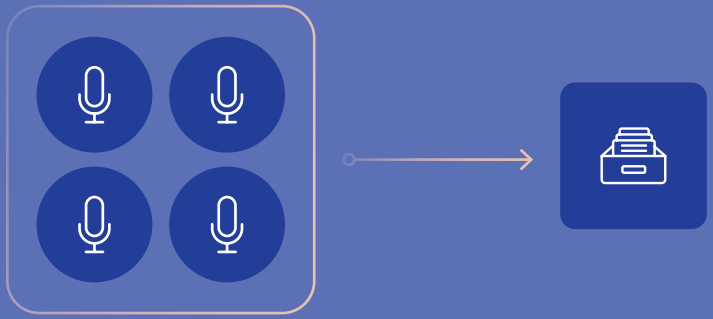
Records management is a fundamental part of compliant data protection. A GDPR-compliant corporate environment, where records containing personal data are routinely identified, classified, protected, and life-cycle managed, relies on mature records management procedures and systems.



Legal obligations and data retention

Consent, like Legal Obligation, is another of the legal bases outlined in Article 6.

Customers cannot opt-out of record-keeping when an organization has a legal obligation to keep records, and contrary to popular belief, there isn't a requirement to obtain consent before personal information is used for business purposes. 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.



Consent is also linked to a third legal basis: Performance of Contract.

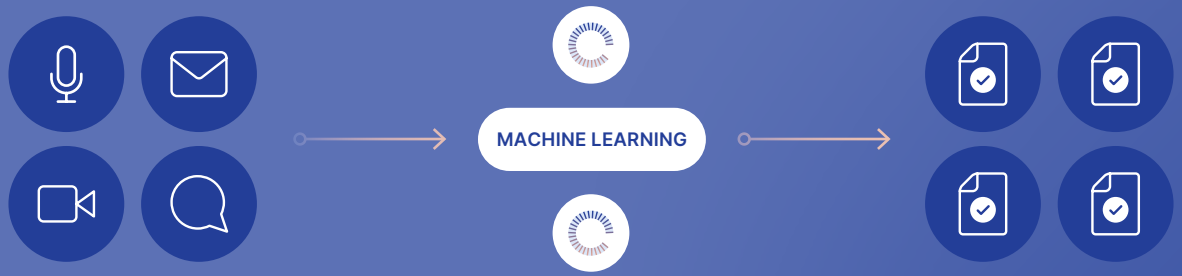
Contracts with investors that lead to a financial transaction are considered business records under MIFID II and require recordkeeping compliance.

This will often involve recording phone calls and retaining emails and other relevant digital communications (dComms) data, and crosses over with obligations under the Market Abuse Regulation (MAR), another significant slice of financial services legislation.

The size and complexity of GDPR, MiFID II and MAR make it impossible for businesses to remain compliant through manual supervision of data processing alone, and an effective compliance program should identify solutions that address these needs with minimal human intervention.

Intelligent communications surveillance tools today can capture this data and apply machine learning to filter out PII where necessary for the purposes of an investigation, minimizing the need for human intervention wheresensitive data is concerned. Many financial organizations have moved on to systems that can comprehensively capture data, preserve its integrity, and apply automated solutions to ensure PII is not accessed.

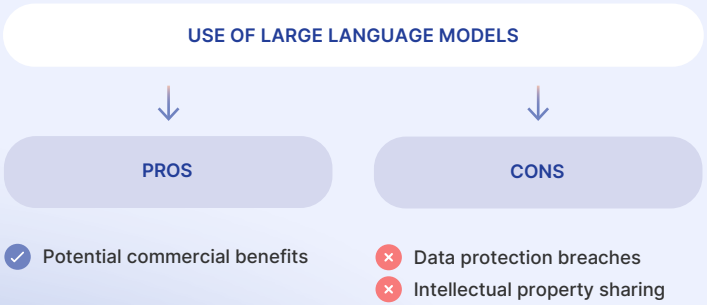
Machine learning solutions can also gather data from an individual's communication behaviors and use algorithms to assess the chances of a problem. Using AI, they can assign a rating and provide benchmarking information to demonstrate where an individual sits in the risk assessment spectrum.



GDPR and Large Language Models: 2023

The rapid evolution of AI and various offshoots like Large Language Model (LLM) chatbots, which rely on using individual data to create behavior prediction models, is one of the great data privacy challenges of the modern era.

As the underlying machines learn from the actions of an individual and the data produced, the predictive power of the algorithm grows. And as AI becomes adept at anticipating individual thoughts, the line between the convenience provided by the internet and other data-collection platforms and their ability to modify behavior vanishes.



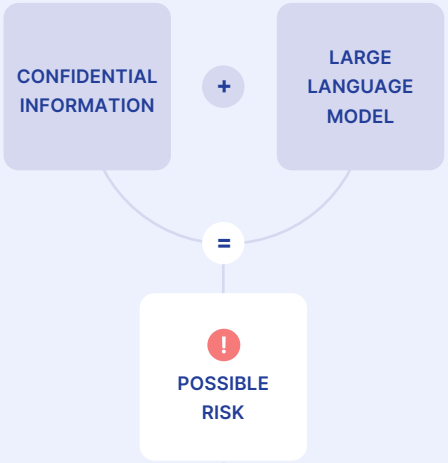
"Not withstanding the potential commercial benefits of this technology, and in common with other tech advances over the years, there are potential legal issues that may arise from the use of LLMs, particularly from an intellectual property or data protection perspective," said Chris Holder, data privacy specialist at law firm Bristows.

While accuracy and efficiency increases with greater amounts of data fed to the machines, so do the chances of data protection issues, he said.

“For example, if datasets created for use by an LLM contain personal data, the relevant data subjects may not have consented to the processing of such data, contrary to the GDPR,” Holder added.

“Further, it is unclear how the ‘right to be forgotten’ under the GDPR would be enforced against an LLM. Whilst it may be possible to remove personal data from content generated by an LLM, it may be practically impossible to remove all traces of an individual’s personal information from the initial dataset used by the LLM to create such content, particularly if the dataset in question is an enormous online word repository such as Wikipedia.”

Firms must be particularly careful that employees handling data that contains confidential information, like trade secrets or financial data, as if entered into an LLM it could be at risk.



Best practices

dComms audit

Thorough auditing of dComms capture and recording practices is essential for compliance, risk management, and maintaining the integrity of PII. A typical audit begins with a clear definition of the objectives and scope, such as ensuring compliance with regulatory requirements like MiFID II or Dodd-Frank, and assessing data integrity.

- **STEP 1** Objectives and scope definition
- **STEP 2** Regulatory requirements and industry standards review
- **STEP 3** Data mapping exercises
- **STEP 4** Data capture processes evaluation
- **STEP 5** Firm's ability to retrieve and search electronic communications records test

Data mapping exercises follow where a comprehensive inventory of eComms and aComms channels used within the firm are mapped, which allows the team to follow communications data as it flows through the business and into storage.

An evaluation of the data capture processes will ensure that all the required channels are covered, coverage of continuous and unaltered.

The firm's ability to retrieve and search electronic communications records efficiently is also tested, along with search functionality, before the team assesses data encryption and security measures. This step ensures the proper measures are in place to protect sensitive information and PII during capture, transmission, and storage.

Recordkeeping and documentation practices are analyzed, including audit trails and change management logs, to ensure records are complete and held in a secure manner.

Compliance monitoring and reporting takes place, along with testing and sampling to verify the accuracy and completeness of the eComms and aComms data. This allows any compliance issues to be flagged for potential shortfalls in regulatory standards.

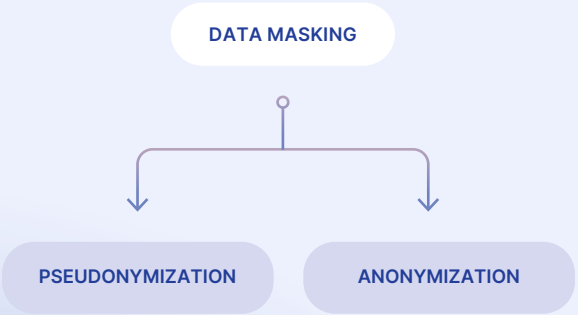
Training and employee awareness steps must be carried out regarding dComms capture and recording policies and procedures. Remediation in recent enforcement actions against businesses that allowed traders to use WhatsApp and other unmonitored chat apps, involved teaching supervised individuals the importance of not using their own devices, or other unmonitored channels, to trade.

When the audit results are fed back to management, compliance gaps, deficiencies, or areas for improvement are identified and addressed. Processes for ongoing monitoring and periodic audits are established to ensure sustained compliance and improvement in eComms capture and recording practices, and following a review by the legal and compliance functions, a final report and certification of compliance is issued.

The role of data masking

In order to meet the seemingly conflicted data protection accountability and financial regulatory obligation demands, data masking is often employed as part of surveillance.

The most commonly used methods are pseudonymization and anonymization. Pseudonymization replaces personal data with an artificial identifier that cannot be used to identify an individual by appearance. Links to the original personal data are maintained elsewhere and allows a theoretically safe reconnecting of an individual to a data record.



Firms using this method with communications surveillance tools for any applicable reason will require the original content records to be correctly archived with pseudonyms intact, along with the mappings that can be used to reconstruct the identity of the masked persons.

The strict standards inherent in MiFID II require the identification of parties in financial transactions for reasons we identified earlier. Anonymization, meanwhile, involves 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 a risky practice for financial services firms, as the content surrounding a transaction may need to be reported to a regulator.

Where anonymization is useful is in secondary situations where Big Data and AI are applied solely to financial transactions for the purpose of business insights.

GDPR and dComms surveillance

A robust compliance framework is essential for organizations to uphold ethical guidelines and ensure employees maintain the highest standards of integrity and accountability.

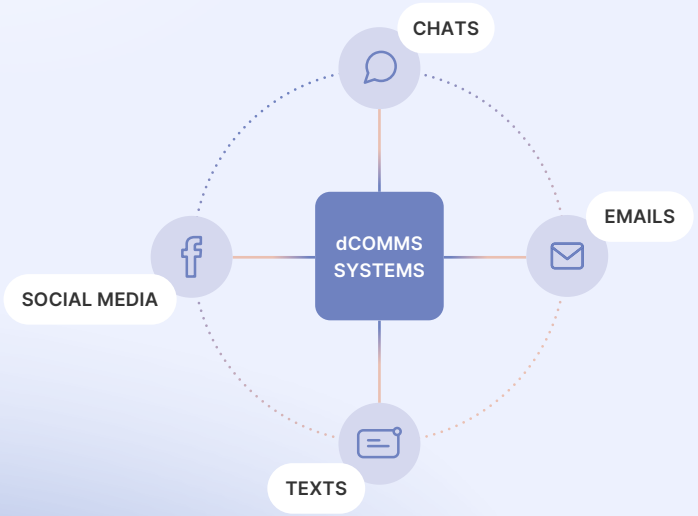
For financial institutions, an intelligent solution for monitoring digital communications is a vital component to meet GDPR regulations as well.

The evolution of AI-powered surveillance technology has also occurred during an era of enhanced data privacy concerns, which creates a conundrum for financial services firms. Regulators are increasingly pushing firms to use sophisticated monitoring programs that combat market manipulation, fraud, money laundering, and other forms of misconduct. While GDPR centers mainly on the collection and processing of customer data, it also covers personal information obtained from employees. More advanced monitoring programs will naturally ingest more data, which can bring several challenges and make GDPR obligations tougher to meet.

Privacy rules also vary across borders, which adds complications to broad data privacy frameworks which have to take into account variances in regulations. The expectation from industry watchers adds complexity for multinationals over time as US states develop their own GDPR-like systems, and various emerging jurisdictions adopt similar guidance.

Financial regulators have not handed down prescriptive rules for dComms surveillance, instead giving guidance amid broader supervision obligations necessary to prevent misconduct.

Effective dComms systems ingest enormous amounts of data from chats, emails, texts, social media from employees across the world. Regardless of the surveillance model used, lexicon- or behavioral-based, random sampling, or a mix of the three, it is inevitable that PII will feature in the captured messages.



IT IS CRITICAL TO UNDERSTAND

- Personal data can only be collected for certain specified purposes.
- Only necessary and relevant information can be collected and retained.
- Monitoring programs must have clearly defined scopes.
- Information gleaned through surveillance cannot be used beyond the legitimate purposes previously disclosed to employees.

Conclusion

Business, society and communications have all evolved considerably since GDPR entered force, changing the way enterprises use and handle data. What hasn't changed is the need for strong information governance and compliance procedures.

Firms that fail to implement proactive policies and procedures in their compliance programs are particularly vulnerable. Areas of data systems, information governance, and procedures for managing electronic evidence in surveillance will continue to be impacted as regulators set case precedents in the coming years.

Building a dComms surveillance solution that balances regulatory expectations with privacy requirements requires careful planning and analysis, and the help of expert partners who understand the role of AI in the current data privacy environment. Intelligent capture and analytics solutions can help forward-thinking firms meet both the demands of financial services data retention rules and GDPR's data protection guidance by reducing the need for human intervention and delivering truly holistic compliance.

To learn more about the only true end-to-end compliance solution, watch our demo at www.shieldfc.com