



SILVERLAKE MASTERSAM INDUSTRY SOLUTIONS INSURANCE

Released 2024

This paper aims to explore how Privileged Access Management solutions from Silverlake MasterSAM can effectively address the Cyber threats faced by Insurance industry

PAM for Insurance Industry

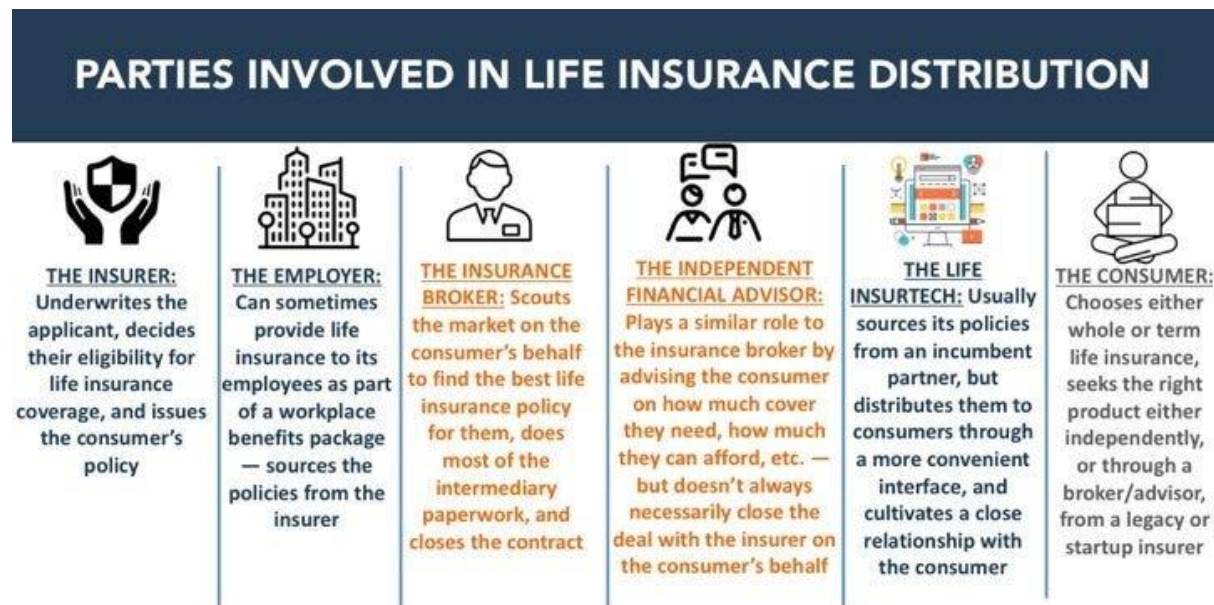
This document, for all intents and purposes, is meant for interested party with special approval and internal circulation purpose. Discretion is required for any external circulation as the information contained within may vary from actual product and may change overtime.

Contents

Nature of Insurance Industry	2
What is GDPR?	3
Why GDPR had high impact for Insurance companies?	3
Implications of non-compliance of GDPR:	3
Key challenges faced in Insurance agencies/ Companies:	3
> Data Portability	3
> Consent Management	4
> Third-party vendor management	4
> Transparency Third Parties	4
> Fraud	4
How MasterSAM can help?	6

Nature of Insurance Industry

The insurance industry protects one from the impact of a financial loss, which can lead to various kinds of perils. The industry is composed of insurance carriers (also known as insurers), insurance agencies and brokerages. Commonly, these insurers are large companies that provide insurance and assume the risks covered by the policy. While some of these large companies are directly related to a specific insurer and sell only particular insurer's policies, many others are also independent and offer variants in the market. Besides offering the primary insurance packages, the industry also comprises establishments that offer insurance-related services, such as claims adjustment or third-party administration of insurance and pension funds.



As insurance companies deal with or transact with a lot of customer data and intellectual property data, they unavoidably become high-value targets for malicious cybercrime actors. A small slip in maintaining a positive reputation in the industry is enough to jeopardize the trust the customers have in the establishment. It is thus, only the companies that have kept themselves away from the news headlines who have enjoyed a better or more competitive edge over the other companies. Besides being a prime target for cyber-attacks, insurance companies also face shortage in skilled security professionals to safeguard their enterprise.

With daunting cyber threats looming, insurance industry also faces the challenge of complying with the numerous compliance and regulatory standards. A regulatory standard that had high impact on Insurance companies is General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

What is GDPR?

The GDPR effective 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive, imposes new obligations and stricter requirements on all organizations involved in the processing of personally identifiable data, emphasizing transparency, security and accountability.

The primary objectives of the GDPR are to:

- Institute citizens' rights in controlling their personal data
- Simplify the regulatory business environment by adopting a unified regulation across the EU

Why GDPR had high impact for Insurance companies?

Owing to the vast volume of personal data and confidential personal data processed by insurers, the implementation of the GDPR would have a substantial effect on the insurance industry. Insurance firms will need a better understanding and command of the information they process and exchange and will also need to be able to explain why the data in question must be collected and kept. Insurance firms will also have to deal with the possibility of exchanging personal data on some circuits with rivals or competing firms.

Implications of non-compliance of GDPR:

Insurers who fail to comply with GDPR regulations face fines of up to €20,000,000 or 4% of total annual global turnover (whichever is greater), organisation reputational risk and individuals are also empowered to bring private claims against organisations where their data privacy has been infringed.

Key challenges faced in Insurance agencies/ Companies:

1. Data Portability
2. Consent Management
3. Third Party Vendors Management
4. Transparency Third Parties
5. Fraud : Many insurers continue to grapple within their industries to detect and reduce both hard and soft insurance fraud, an issue that costs the sector \$80 billion annually.

> DATA PORTABILITY

A significant challenge confronting the insurance industry is the implementation of data portability as mandated by Article 20 of the General Data Protection Regulation (GDPR). This provision grants individuals the right to obtain their personal data, which they have provided or which has been observed, in a structured, commonly used, and machine-readable format. Furthermore, it allows them to transmit this data to another data controller without hindrance.

> CONSENT MANAGEMENT

Consent is a tricky challenge for insurers in the context of GDPR as it related to processing of special personal data. According to GDPR, consent can no longer be implied, it must be freely given, specific, informed, unambiguous, clear affirmative and no imbalance of power must exist. Health data is considered sensitive and collecting it is obviously vital to underwrite and perform numerous types of insurance contracts.

Despite much lobbying by insurance establishments to incorporate an additional basis for processing sensitive data specifically for insurance purposes, currently under the GDPR explicit consent appears to be the only legal basis for insurers to process sensitive data. This poses a particular problem for sensitive personal data on the current book of business where no consent was received historically. And, addressing this concern is going to be particularly challenging and very time-consuming.

> THIRD-PARTY VENDOR MANAGEMENT

Insurers will need to look at arrangements they have with third parties (such as vendors and brokers) to determine if this is controller-to-controller or controller-to-processor relationship. The level of control over the data and whether the entity is involved in decision making relating to the personal data should be discussed.

It is probably the brokers who will be classified as controllers but the insurer must analyze this on a case-by-case basis to determine this. It will be important to review and accordingly amend contracts and agreements with controllers and clearly spell out the split in compliance responsibilities to avoid dispute in the case of a data breach.

> TRANSPARENCY THIRD PARTIES

One of the major challenges emerging in the insurance industry is the requirement under Article 14 to provide information where personal data has not been obtained from the data subject. This means where data has been received from a third party, the data subject to whom the personal data relates will now need to be informed of certain details regarding the processing within a set timeframe.

> FRAUD

Most state insurance regulations require insurers to document and submit their antifraud plan to the state's department of insurance. Although companies have documented antifraud plans, do they know how effective they are? Insurers should manage against several different types of fraud threats from cyber risk to employee theft.

Traditional fraud management typically handles business risks in silos: a fake customer account here, a padded claim there. It's an inefficient model that is not able to quickly counter evolving fraud schemes and behaviors.

A modernized approach using advanced analytics—whether through real-time, near-term dynamic, or longer-term scanning for emerging threats—can help a company respond to gaps in current processes and/or improve controls and monitoring for fraud. Key capabilities include:

- Anomaly detection
- Machine learning
- Text or voice analytics
- Network analytics

A new approach to enterprise fraud management can provide organizations with many benefits, including high-value risk insights that can be used to dramatically improve operational and strategic decision-making.

As they evaluate the different regulations and introduce steps to meet insurance regulatory criteria, insurers will likely face major strategic and operational decisions. Impacts are likely to span several areas, including:

- Service deals
- Review of disputes
- Producer compensation and incentives
- Various disclosures for consumers
- Documentation to endorse feedback from producers
- Policies, processes, control systems, and recordkeeping for oversight and compliance

How MasterSAM can help?

Insurers have spent a lot of time and money preparing to comply with the European Union's General Data Protection Regulation and the California Consumer Privacy Act. But have they done enough? Looking ahead, organizations need to also brace themselves for additional insurance regulatory initiatives.

Many insurance companies are struggling to meet new insurance regulatory requirements because their siloed legacy systems lack integration. The overwhelming volume of data being maintained can also be a problem. Insurers should consider establishing a more comprehensive information governance program that addresses these and other data management and privacy challenges, not just to meet compliance standards, but also to enable better business decisions and actions. Potentially helpful approaches include:

- Using data minimization, which involves setting protocols to automatically flush superfluous information on a regular basis
- Increasing engagement with customers to better utilize all the new data at their disposal
- Asking questions about current data and privacy governance: What and where data about specific consumers is being stored, how complete and accurate it is, and how it is being used and protected

Learn about how a comprehensive and coordinated approach to information governance can effectively help organizations to tackle privacy issues.

- Review any gap analysis and any risk assessment completed to date between your company's existing data protection processes and the GDPR;
- Help create and collate personal data registers;
- Assess your company's GDPR Readiness state;
- Identify weakness and help your company work through any problematic or high impact areas;
- Work with your company to put a detailed project plan in place to ensure compliance ahead of the deadline;
- Assist with the design and implementation of revised data protection governance structures;
- Help with the roll out of staff training and awareness throughout the business; and
- Assist with the implementation of an ongoing monitoring program to demonstrate compliance.