**SecuPi**

# Customer Use Case
## Groupama Italy

A flexible and scalable approach for de-identifying and protecting customer data on cloud & on-prem while meeting GDPR Right to Be Forgotten requirements

# About Our Customer

Groupama is a leading mutual insurance provider of life, auto and property insurance with over 12 million customers and 14.4 billion Euros ($16 billion USD) in annual premium revenue. Groupama needed a comprehensive, easy-to-implement solution for managing and protecting Personally Identifiable Information (PII), while complying with challenging GDPR requirements across all lines of business.

# The Challenge

As a mutual insurance group, Groupama needed a solution to protect data for its millions of customers and members across multiple organizational business units, technologies, user communities, and more.

Groupama was aware of the significant amount of personal and sensitive data within its different databases, data repositories, and applications. This data was scattered across multiple data repositories, accessed by many different users, from different business units, with different business needs, using different technologies directly or through CRM and other applications. Different data access control policies had to be enforced based on any number of User or Data attributes including User location, Role memberships, Data Subject preferences, Geo-Location, Access Method(s), etc.

This required a wide range of data security and privacy compliance capabilities including Data Anonymization, Masking, Consent Management and Right to be Forgotten (RTBF) to address safe personal data access, both for security purposes and GDPR compliance requirements. Business continuity had to be assured without complex changes to business processes and without disrupting day-to-day business processes.

The customer had several non-production environments that were used for development, testing, and analytics that were replicas of production environments. The personnel handling these non-production environments were mainly analysts and developers, who were unauthorized to access personal customer data contained in these environments. Groupama wanted to grant access to authorized users only in order to maintain data access on a need-to-know basis across all the organization and they sought a solution for de-identifying data for unauthorized users.

An especially challenging requirement that the customer was facing in the process was to properly handle the GDPR Right to Be Forgotten (RTBF) requirement, while during and after the retention period. While the RTBF article requires organizations to delete customer data upon the customer's request, there is also a retention period of 7-10 years after the deletion request, during which data also needs to be preserved for legal and tax purposes. After the retention period, the data has no legal basis and hence needs to be deleted. Reconciling these two requirements was challenging and required both a strategic approach and a flexible technical solution.

> An especially challenging requirement that the customer was facing in the process was to properly handle the GDPR Right to Be Forgotten (RTBF) requirement, while during and after the retention period.

## Important Considerations

As a leading Insurance group, offering life, auto, property and other insurance products to millions of customers, Groupama required a data privacy solution with the following capabilities:

1. **Flexibility** - Provide flexible, fine-grained data remediation capabilities including dynamic masking and FPE encryption.

2. **Manage Complex Rules and Environments** - Manage multiple overlapping hierarchies and matrixed data access control policies for different user roles based on complex rules managed centrally across Groupama's IT technology stack for regular and privileged users.

3. **Real-time Visibility** - Provide real-time visibility into data consumption and data access with real-time analytics capabilities, forensics, Security Center integration and no code changes to existing databases, infrastructure or applications transparent to user's day-to-day business processes.

4. **Integrity and coherence** - Maintain referential the integrity of the data within the database and integration between applications. A customer ID that, based on the contractual relationship it has with Groupama, is managed consistently among all the applications of the project perimeter

5. **A Centralized Platform** - Single platform to manage access, data privacy and regulatory compliance across Production and Non-Production environments for different user communities (e.g., Testing, QA, DBA, Business Users, etc.).

6. **Safe Deletion Methods** - Enable 'Right To Be Forgotten' enforcement with Logical Deletion on Production and Non-Production environments while addressing other data retention regulations.

7. **Avoid Compromising Data Integrity** - It was important that the data deletion would not modify data in the anonymization process, to prevent compromising the data integrity. The platform should be able to prevent an unauthorized user from being able to modify or delete data on the interface by blocking such operations.

8. **Maintain Performance and Business Operations and** - The solution could not negatively impact performance and business operations.

Groupama chose SecuPi as its protection solution as it delivered robust data governance, privacy compliance and policy enforcement is through fine-grained Attribute Based Access Control (ABAC), Anonymization, Encryption and Dynamic Masking.

## The Solution

After trying multiple solutions on the market, Groupama Italy chose to use SecuPi for protecting sensitive and personal data on their business applications.

A joint effort of **Brinthesis**, for system integration and project management expertise, and **SecuPi** for developing and providing a single, centralized protection platform.

## Highlights

- Flexibility and Scalability

- Minimal impact on business operations and performance

- One central solution for a variety of applications, tools and use cases maintaining data integrity and consistency among all the applications

Groupama chose SecuPi as its protection solution as it delivered robust data governance, privacy compliance and policy enforcement is through fine-grained Attribute Based Access Control (ABAC), Anonymization, Encryption and Dynamic Masking. This allowed Groupama to provide on a 'need to know basis' data access to sensitive data for authorized users only, across various applications and data consumption tools used by different users and job functions within the organization. A centralized data access control platform providing a single pane-of-glass that does not require code changes, development effort or business process changes is a key component of any solution enabling practical data governance while supporting different trust models.

SecuPi's solution allowed Groupama to apply data governance, data protection and privacy compliance across its entire IT ecosystem and user communities within days with no code changes or development effort.

SecuPi's unique approach to data protection and compliance provides Groupama with a simple, centralized platform, governing data access control, data encryption/ decryption, dynamic masking, filtering, geo-fencing and/ or data obfuscation operations managed by policy from a single Central Policy Management Server. Full data mobility is ensured when access control and data protection policies or rules follow the data regardless of the data repository or application used to access the data supporting future Groupama initiatives.

SecuPi's solution allowed Groupama to apply data governance, data protection and privacy compliance across its entire IT ecosystem and user communities within days with no code changes or development effort. SecuPi's unique approach to data protection and compliance provides Groupama with a simple, centralized platform, governing data access control, data encryption/ decryption, dynamic masking, filtering, geo-fencing and/ or data obfuscation operations managed by policy from a single Central Policy Management Server. Full data mobility is ensured when access control and data protection policies or rules follow the data regardless of the data repository or application used to access the data supporting future Groupama initiatives.

## The Deployment

A rapid and incremental approach was required for the implementation. Groupama needed to establish a full audit trail and accountability for all access to PII. Then, immediately start adding access rules to restrict or block any unauthorized access followed by limiting access for authorized users on a need-to-know basis and ending with fine-grained controls and dynamic masking for privileged System Admin, DBA or Data Analyst access to the databases or applications used to access the sensitive data.

Fully redundant SecuPi components and Central Policy Server(s) implemented using standard Docker container configuration.

## The Result

Groupama built a robust, flexible and scalable foundation for securing their customer data across multiple environments, both internally in pre-production environments and externally in non-production environments. This foundation allows the company to continuously and flexibly scale data protection on additional tools and applications.

Groupama successfully fulfilled its security and compliance goals:

- Customer data was protected, on-premise and in the cloud, both on non-production and production environments

- Comply with GDPR "Right to Be Forgotten" Requirements, while meeting Retention Period demands

- Maintaining the integrity of the data across applications

- Ready to scale across additional environments with several more applications in the roadmap