CASE STUDY

ADIS COMPLIES WITH GDPR, IMPROVING EFFICIENCY AND RELIABILITY OF DATA ANONYMIZATION USING DOT-ANONYMIZER

Interview with Gaëlle Jonckheere: Operational IT Manager / Infrastructure and Applications

ADIS

Customer

ADIS is an insurance brokerage company with a specific focus on life and health insurance. The company is a subsidiary of both AXA and AGIPI's contract management center.

ADIS was founded in 1981 and currently manages over 700,000 insurance contracts. It is headquartered in Alsace, France and employs over 400 staff. ◆

Context

To comply with the new GDPR constraints, ADIS faced the challenge of anonymizing its customers' personal data. For greater efficiency and reliability, they sought a solution to automate this process.

Which were your specific confidentiality constraints around personal data?
The confidentiality of personal data is the subject of continuous concern for the insurance sector.
ADIS is fully committed to compliance with confidentiality regulations and the organisation places a very high priority on the integrity of our processes to manage our customers' data.

In your context at ADIS, how would you define personal data?
Personal data is any data that can identify individuals directly or indirectly. For example, social security numbers, correspondence details (Address, Email, Phone numbers) and details of the products which specific clients purchase from our organisation.

How did your data anonymization requirements evolve?
We decided to revisit our anonymization policies as early as 2016, with the emergence of the GDPR. The subject has been part of our ongoing Security and Data Protection policies since we began trading but the new GDPR regulations allowed us to refresh our processes and we began to actively evaluate solutions to meet our requirements.

After examining the solutions available, we selected DOT-Anonymizer from ARCAD, which offered us greater security than the pseudonymization solutions on the market. ARCAD offers both superior data anonymization techniques and ensured our organisation can safely combine two distinct sets of data without any risk of identifying an individual.

What impact does the GDPR have on ADIS?
Prior to the GDPR coming into force, we worked on researching the implications for our specific business and informed our teams on the potential impact on our processes.

The GDPR cites pseudonymization as a reliable and effective means of protecting data. However pseudonymization allows for the original data to be revealed under certain conditions, a potential gap in most standard security processes which ADIS needed to ensure was eliminated.

Instead of pseudonymization, we opted for ARCAD's irreversible anonymization, which gives us a greater level of security to guarantee that it is impossible to retrieve the original data value.

Another advantage of DOT-Anonymizer was the ease of configuration for our specific anonymization requirements. Settings can only be accessed by certain authorized profiles. The solution's profile management allows us to lock down our security policy.

Why did you select the DOT Anonymizer solution?
There were 4 main reasons for our choice:

1. DOT-Anonymizer was one of only a few solutions on the market able to meet our strict anonymization requirements.

2. DOT-Anonymizer is entirely DBMS-agnostic as it is written in Java. It is compatible with any database that has a Java Database Connectivity driver (JDBC), like SQL Server, Oracle, MySQL, DB2, PostgreSQL, Sybase, MongoDB. It can also handle .xml and .csv files.

   Thanks to DOT-Anonymizer, we can centralize all our anonymization rules in one single solution, which ensures data consistency and integrity across databases of different types.

3. DOT-Anonymizer supports "homonymy", meaning the same item of data is anonymized in a consistent way across all our databases.

4. We received positive feedback DOT-Anonymizer from another customer, Banque Palatine, who were already running the solution in production, which helped to confirm our choice.

How long did the anonymization project take?
Our very first discussions around the data anonymization project started in May 2016. A "pilot" project was implemented between November 2016 and February 2017. We then refined and extended the anonymization rules across other areas of the system and transferred these to production in September 2017.

How was the anonymization project run?
Our preferred vendor, ARCAD Software, managed the implementation and configuration of DOT-Anonymizer in collaboration with ADIS teams. ARCAD has been particularly attentive to our specific needs. For example, we needed to ensure consistency between postcodes and city names, and ARCAD provided a Groovy script to cover this particular requirement. This scripting technique makes the DOT-Anonymizer solution very flexible and suitable even in the most complex and specific business use cases. It is easy to extend the default DOT-Anonymizer engines in a very powerful but also maintainable way.

The implementation of the ARCAD solution was flawless. As a vendor ARCAD was very reactive and always available, which was important to us because of the high profile which this security project had at the highest level of our management.

How easily was DOT-Anonymizer adopted by your Team-members?
Before we started, our teams feared that integrating a data anonymization solution into our system would increase their workload and change their working methods.

They were also concerned about losing end-to-end test continuity.

However, once DOT Anonymizer was installed, these fears were rapidly allayed, and the teams appreciated the value and ease-of-use of the solution.

The testing team found that there was very little impact on their processes. Because DOT-Anonymizer preserves data type and format, the anonymized data remains usable for testing purposes allowing our QA Team to find the most complex "edge case" defects which tend to be the most difficult to fix.

I would recommend involving operations staff, testing and development teams right at the start of the anonymization project in order to ensure a seamless adoption of the automated solution.

What is your feedback on DOT Anonymizer after several months of use?
We are very satisfied with DOT-Anonymizer, the solution has lived up to our expectations.

It is important to keep in mind that whenever a data anonymization solution is integrated into an information system, the anonymization phases must be automated and planned, in order to refresh environments regularly. The solution must also be tuned according the system scope and interact with other system and security tooling.

What are your next projects planned?
Our next step will be to put in place a methodology using DOT-Anonymizer to immediately identify whether new data entering the information system needs to be anonymized, and how, to remain consistent with other similar data. This way we will automatically discover data that needs to be anonymized and integrate it with the ongoing anonymization process. ◆

> " ADIS teams were quick to see the value and ease of use of DOT-Anonymizer. Our testers were very quickly up and running with the solution, thanks to the guaranteed consistency and integrity of anonymized data, across all our DBMS. ARCAD Software staff were particularly responsive to our specific needs. "
>
> *- Gaëlle Jonckheere*
> */ Operational IT Manager*
> */ Infrastructure and Applications*