OCTOPAI

GDPR is all about knowing where your privacy sensitive data comes from, where that data resides within your systems, and proper data management - with particular focus on metadata management as the key to compliance.

GDPR CASE STUDY 1: LOCATE PRIVACY SENSITIVE DATA INSTANTLY

Background

GDPR demands that companies processing sensitive personal data of European residents take additional measures to ensure protection of said sensitive data. A large part of this pertains to access - giving people access to their own personal data, enabling portability of the data, changing or deleting the data.

Before any company can allow access to personal data, it must first locate the sensitive data. Let's take credit card columns for example.

The Challenge

A Business Analyst in a large insurance company must identify every single place customer credit card columns reside inside the company's reporting systems. Once he does so, he will need to either eliminate the credit card number column from the report or mask the data inside the column so as to protect this data's security and comply with GDPR.

Before Octopai

Finding every single location credit card columns exist within a company's reporting systems is a ton of work and can take a really long time. The Business Analyst has to consult with multiple different IT functions in order to understand how to conduct his manual search for the sensitive data required, and must pay close attention to impact of any potential change to the column. Not a simple task.

Octopai automation easing GDPR compliance

With Octopai, this entire process is automated. BI groups can **auto-discover, access and retrieve metadata in seconds.**

The Business Analyst simply has to enter "credit card" into the search field, and even if this is not the exact name of the column (sometimes the column name differs slightly - credit_c or c_credit, for example), Octopai maps out all the reports related to this specific sensitive data, and instantly locates everywhere the credit card columns resided within every single reporting system. He then was able to perform the data masking required in order to comply with GDPR.