

## CASE STUDY

# International Bank Secures Cross-Border Data

In order to streamline operations and improve analytical capabilities, a major international bank chose Protegrity to remain compliant with data-privacy regulations when they consolidated all European operational data from various European bank entities to their Teradata enterprise data warehouse (EDW) at their headquarters.

## KEY HIGHLIGHTS

### CHALLENGE

Protect personally identifiable information of customers across multiple systems to the satisfaction of EU cross-border data privacy requirements.

### SOLUTION

Deployed Protegrity Privacy Protect with vaultless tokenisation locally, to de-identify new and existing PII at source banking entities (before transfer to headquarters), and Protegrity Database Protectors on the Teradata enterprise data warehouse at headquarters.

### INDUSTRY

Banking & Financial Services

### IMPACT

End-to-end, fine-grained PII de-identification across all geographically distributed bank entities to meet all EU cross-border data privacy requirements, including country-specific data access restrictions.



## OBJECTIVES

- Consistently secure the large amount and variety of personally identifiable information (PII) of customers – including names, addresses, phone, email, policy and account numbers – across multiple systems, end-to-end from the geographically distributed bank entities, back to headquarters, where it would be consolidated.
- Protect existing data within all systems.
- Maintain compliance with EU cross-border data protection laws, including the Federal Act concerning the Protection of Personal Data in Austria (Datenschutzgesetz 2000 - DSG 2000) and the Federal Protection Act in Germany (Bundesdatenschutzgesetz), which require that access to Austrian and German customer data at headquarters be restricted to only users in each respective country.

## CHALLENGES

- Need for centralised data control with local data management for consistent security and auditing across all entities.
- Security must be compatible with multiple data types from a variety of systems, including SAS, Mainframe and ERP.
- High throughput to ensure maximum reliability and data integrity.



## SOLUTION

The bank implemented the Protegrity Privacy Protect solution, to locally de-identify new and existing PII with vaultless tokenisation at the source of banking entities before transfer to headquarters. Protegrity Database Protectors on the Teradata EDW at headquarters ensure both compliance with EU cross-border data protection laws and complete business analysis capabilities. Protegrity's vaultless tokenisation was delivered via clusters of multiple servers to maximise throughput with bulk tokenisation.

In addition, centralised policy-based access controls were implemented with integration of both Lightweight Directory Access Protocol (LDAP) and Active Directory. This restricted access to re-identified data to authorised users, including country-specific requirements for Austria and Germany.

## IMPACT

Utilising Protegrity's Database Protectors and vaultless tokenisation with centralised policy, key management, auditing and reporting (delivered via Protegrity's Enterprise Security Administrator), the bank achieved end-to-end data privacy and was able to secure all new and existing PII across their business entities with complete, fine-grained de-identification of sensitive data



## BUSINESS VALUE

- The bank can centrally manage the security of sensitive data regardless of where it goes, including control over information associated with persons from Austria and Germany – the security team at headquarters can prevent users from accessing sensitive information associated with persons from each respective country.
- The flexibility of the solution provided a means to protect the wide variety of data types necessary across multiple environments, while maintaining maximum throughput, reliability, and data integrity.
- Unified controls provide increased security, simplified compliance and superior oversight, along with the added protection of a built-in separation of duties.
- Met all EU cross-border data privacy requirements, including country-specific data access restrictions.

## TECHNICAL VALUE

- Tokenisation was selected to protect the PII, due to its high performance and transparency, in addition to its benefits in cross-border law compliance.
- Rather than encryption, which uses a cipher/key system reliant on a mathematical algorithm, tokenisation replaces sensitive data with random data of the same type and length. Because there is no mathematical relationship to the original data, tokenised data is considered replaced or removed, and therefore secure.
- The unique architecture of Protegrity's vaultless tokenisation technology provides all of the benefits of tokenisation without the drawbacks and limitations of traditional tokenisation; no ever-growing token lookup tables and no replication, which can seriously affect performance, and most importantly, no stored sensitive data.



## WHY PROTEGRITY?

For more than two decades, Protegrity, a global leader in data security, has protected the sensitive data of the largest brands in the world, including four of the world's 15 largest banks and three of the world's leading multinational companies. Protegrity provides the only platform that lets enterprises decide which data should be classified as sensitive and allows them to control how they safeguard that data, enabling the bank to securely and compliantly leverage external cloud data analytics. With Protegrity, this international bank has unrestricted enterprise access to all generally available data security technology, both now and in the future, including advisory services and 24 x 7 support.

For more information, visit  
[www.protegrity.com](http://www.protegrity.com)