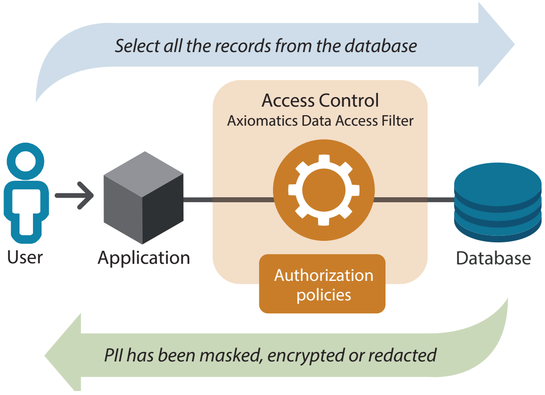
Cross-Border Privacy Enforcement
Global Financial Services and the data flow challenge

Challenges

- **Purpose of data access varies with business process objectives.** Privacy depends on the purpose of use.
- **Controls not adapted to privacy.** Existing business controls focus more on data integrity than privacy.
- **Authorization depending on residence.** Jurisdiction of data subject may apply regardless of data residence and even if data is machine processed only.
- **Reporting tools.** Data warehouse solutions must not bypass master data controls.
- **Master data management.** Sensitive data must be redacted, masked or encrypted depending on the purpose of use.
- **Multi-layered security.** Privacy controls are needed on application, data and network layers.


Select all the records from the database
Access Control
Axiomatics Data Access Filter
User
Application
Database
Authorization policies
PII has been masked, encrypted or redacted

Axiomatics customers benefit from the flexibility of policy-driven authorization combined with data-centric enforcement. Our solutions are used by financial institutions around the globe to manage and enforce user permissions to sensitive data.

Cross-border privacy challenges

Privacy regulations impact cross-border transactions in the financial services industry. Domestic processing of personally identifiable information (PII) and the transfer thereof for storage or processing outside the country's jurisdiction are scenarios with different regulatory mandates.

Privacy is relative to the context. To process a loan application, the loan officer must have access to sensitive personal data about the client. A staff member accessing loan details in a different process phase or situation, may not be authorized to see these personal details. PII authorization by nature depends on the context in which the data is being accessed.

Business controls tend to focus on the correctness and accuracy of data, i.e. the integrity. Privacy adds conditional confidentiality requirements making authorization complicated. There is no one-size-fits-all approach to privacy controls.

Harmonizing privacy regimes

Efforts are being made to simplify business across borders. International agreements that harmonize privacy requirements include:

- The EU Data Directive creates a "European Digital Single Market."
- The APEC Cross Border Privacy Rules (CBPR) "facilitate privacy-respecting data flows among APEC economies."
- The OECD Privacy Framework of 2013 concludes that "flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities."

However, the immediate impact of such collaboration makes things more difficult for multinationals. Harmonization means adapting to the country that has the strictest regime while adding mandates to enable cross-border data flows.

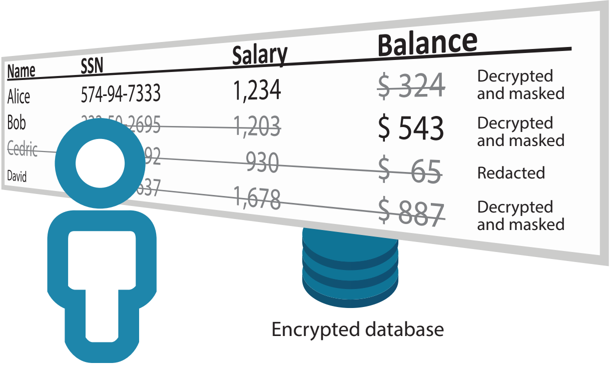
Example: Singapore

Legislators in many countries are constantly introducing new requirements and severe penalties for compliance breaches. Singapore, not yet an APEC CBPR signee, has, with its Personal Data Protection Act of 2012, raised the bar for several Axiomatics clients.

Use case examples

At Axiomatics we encounter a broad range of use cases that relate to cross-border privacy management at our customer sites.

- **Leading European bank stores and processes personal information about Singapore citizens within its data centers in Europe.** To meet the mandates of the Monetary Authority of Singapore (MAS), privacy sensitive data about Singapore nationals must be encrypted in transit and at rest. As a result, data must be decrypted for authorized use, while being redacted, masked or left encrypted if authorization policies based on MAS requirements deny access. Similar privacy regimes also impact the bank and add complexity to policy enforcement.
- **A multi-national financial institute "outsources" data processing to branch offices in a country with lower labor costs.** The flow of PII must be adequately managed which means privacy regimes of all impacted data subjects, i.e. all clients, must be adhered to. Policy-controlled data filtering and data masking techniques need to be combined to meet requirements which span privacy regimes.
- **A large international bank initiates a data warehouse program.** The goal is to improve risk management and internal controls while also enabling more innovative business development. Analysts, administrators and other users of the data warehouse must gain access to underlying databases in ways that keep referential integrity and preserve data formats while ensuring that no PII is revealed. Again, multiple privacy regimes must be adhered to in ways that differ depending on user role and purpose of use.



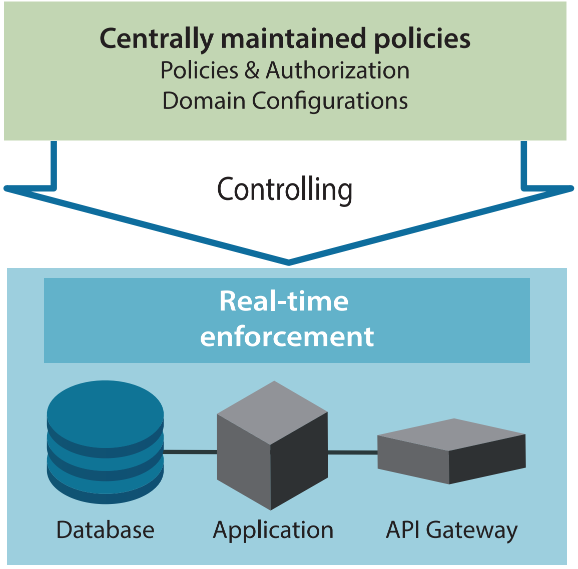
The Axiomatics solution

In our experience, two essential capabilities must be combined to meet the dynamic nature of access control requirements that our customers face in these types of use cases:

- The mandates of multiple privacy regimes can never be "hard coded" into the bank's IT systems, especially since the regulations themselves keep changing and evolving. Instead, they must be expressed in terms of access control policies that uphold business objectives and reflect the legal or regulatory frameworks. The policy constructs must be flexible and easily adaptable as requirements change. They should ideally be maintained at a central point, easily presented for auditing and reporting purposes.
- The enforcement of authorization polices may have to take place on multiple layers: on the application layer, within API gateways and, most importantly, within the data layer. Ensuring that authorization policies are translated in real-time into operational controls to redact, mask, encrypt or decrypt data elements as needed is a crucial aspect of PII protection.

More information

Would you like more information about Axiomatics products or to discuss your use case? Contact your sales representative, or email us at webinfo@axiomatics.



AXIOMATICS Inc
525 W Monroe St #2310
Chicago, IL 60661, USA
Tel: +1 (312) 374-3443

AXIOMATICS AB
Västmanagatan 4
111 24 Stockholm, Sweden
Tel: +46 (0)8 51 510 240

www.axiomatics.com
twitter.com/axiomatics
webinfo@axiomatics.com