EBOOK

PBAC: Evolving Access Control to Cross-border Regulations

Understanding the importance of modern Authorization on controlling enterprise data access for compliance

plainID

Table of Contents

Introduction

Amidst the swiftly changing landscape of cross-border data access and protection regulations, organizations have adopted a more reactive approach rather than a proactive one to ensure compliance. These regulations primarily focus on the secure transfer and access of personal or sensitive data across borders.

Consequently, organizations are forced to make interim modifications to their existing access management and data privacy strategies – a practice that lacks long-term sustainability. Traditional access management methods, such as entitlement or role-based access control, and protection measures like confining data to data center environments or relying on single-tier protection, are no longer compatible with the dynamic nature of these regulatory or customer data processing requirements.

Cross-border data access contains many different regulations and requirements that must be met. In this guide we focus on two important parts:

1. **Global data protection** as the law dictates. For example, "sensitive and private data of German citizens cannot leave Germany."
2. **Data processor requirements** dictated by B2B agreements.

The Data Landscape

Data has exploded in the last two years at an exponential rate and has become the revenue lifeline for many organizations. Without accessible data, businesses grind to a halt. But to make data usable businesses must comply with privacy requirements prescribed by cross-border regulations and B2B and B2C processing agreements.

Navigating the constantly changing regulatory environment, establishing business agreements, and adapting to evolving technological terrains are all part of maintaining secure and compliant data access. These tasks have become a complex challenge that can no longer be effectively handled through our traditional, and siloed access control methods.

Traditional methods to data access control are:

- **Too narrow** in its coverage to ensure all access to data is secure and compliant.
- **Too simplistic** in its access decisioning to meet the fine-grained authorizations requirements.
- **Too fragmented** to be easily manageable and auditable.

What are the Challenges?

There are two key areas to address regarding cross-border access. The first pertains to **global data protection laws** that dictate how, when, and where data can be utilized. Some of these laws require user consent before data can be used, especially in the context of data analytics.

Certain data privacy regulations, like cross-border laws, impact business operations, as they restrict the movement of sensitive personal data outside specific countries. For instance, EU citizen data must only be processed within the EU, and German citizen data should remain within Germany. Compliance with such laws is essential for business operations.

The second aspect involves **data processing agreements** with B2B partners. While some agreements may not be legally mandated, they are compliance requirements set by partners. For example, a US-based bank may require an identity verification company to use only US-based personnel for verifying driver's licenses, even if no law enforces this company policy. Nevertheless, adhering to these processing agreements becomes crucial for maintaining business relationships with partners.

USE CASE EXAMPLE

The Customer:

Fortune Global 500, digital communications technology conglomerate company with worldwide operations and regional customer support teams.

Challenge:

The organization needed a way to control access that addresses local, and global data regulatory compliance and data processing requirements.

The legacy system lacked the granularity and flexibility required to achieve cross-border compliance when handling customer-related data. Without proper access control, the company was at risk of large fines as well as reduced customer acquisition and retention – that would result in revenue loss.

Solution:

Centralized control of authorization policies to define and enforce access to customer tickets and data based on the location of the customer and the support personnel.

Business Impacts and results:

- Efficient approach towards addressing global regulatory compliance
- Increased security and protection of sensitive data
- Improved user experience for workforce employees and customers
- Increased productivity
- Decreased operational costs

What is the Solution?

These challenges boil down to the same subject: **Data Access Control.**

The law does not care if data is made accessible through: Applications, APIs, Microservices or Databases, nor should the solution be put in place to answer how the data is accessed.

This is where **Policy Based Access Control (PBAC)** comes in.

PBAC is a flexible authorization strategy that provides enterprise-wide visibility and control. It does this by externalizing authorization, centralizing the policy management, and distributing its enforcement.

This approach helps enterprises with scalability and achieve faster time-to-market that was not possible before with RBAC and ABAC alone. PBAC draws from previous methods and modernizes authorization by applying a layer for business logic through natural language. Equally important, it makes authorization dynamic, contextual, and risk based.

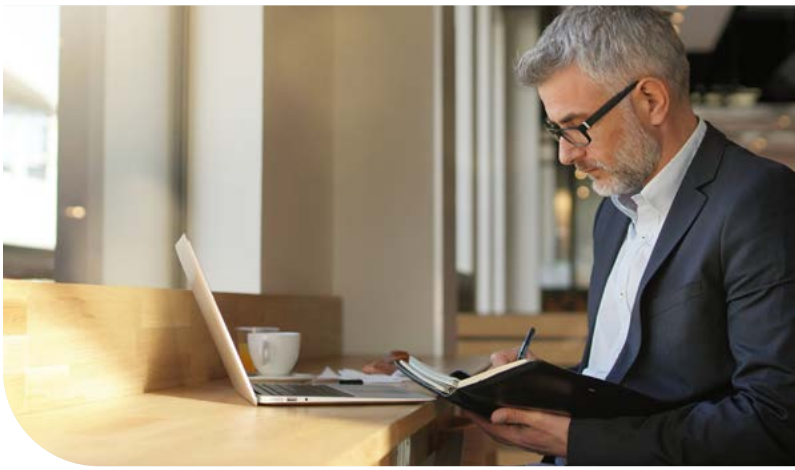
PBAC policies can take a range of factors into account, such as:

- User attributes (e.g., country of citizenship)
- Resource attributes (e.g., country of origin)
- Environmental conditions (e.g., current user location)
- Data in diplomacy (e.g., trust based on geopolitics) and policy rules for cross-border compliance.

This enables enterprises to implement complex access control schemes tailored to their specific security requirements and business needs – both of which rapidly change over time.

PBAC allows organizations to take the complexities of cross-border access from law and agreements to simple manageable natural language policies that can be enforced regardless of whether the data access is through an application, an API, service, or database connection.

Like the nature of regulations, enterprises should not concern themselves with the intricacies of enforcing cross-border access. Instead, their focus should be on determining which policies need to be implemented. PBAC provides the ability to change access policies on the fly, giving enterprises the flexibility and speed needed to keep up with the ever-evolving technological and regulatory landscape.



Does PBAC Integrate with Data Governance Tools?

PBAC solutions offer a powerful mechanism for enforcing data protection, especially when integrated with data catalogs. By leveraging data catalogs, organizations gain a centralized repository that provides a comprehensive view of their data assets, including metadata, classifications, and access rules.

With data catalogs, PBAC can make more informed access decisions based on the contextual information available. The catalog's insights enable PBAC policies to be more nuanced and precise, aligning access privileges with the sensitivity of the data, applicable regulatory requirements, and organizational risk factors.

The **combination of PBAC and data catalogs** empowers organizations to implement fine-grained and adaptive access controls. When regulatory changes occur, these solutions can dynamically adjust access privileges based on the evolving data landscape, ensuring compliance with cross-border data regulations.

Furthermore, data catalogs address region-based data access challenges by providing insight into where the data is stored and the country of origin. Organizations can implement appropriate policies through PBAC to manage and reduce data sprawl while respecting data residency obligations.

By applying PBAC solutions alongside data catalogs, organizations establish a resilient data protection framework. These integrated systems enable businesses to navigate cross-border data regulations more effectively and confidently — fostering a secure and compliant data environment.

How does PBAC help with Data Processing Agreements?

In addition to regulatory requirements for cross-border access, B2B partners contribute to the complexity with their own requirements. Their individual compliance and risk teams may impose specific rules about where their data can be processed, adding another layer of considerations to manage.

While there are no regulatory reasons to adhere to these requirements, enterprises have a business reason to follow such corporate practices. If an enterprise does not comply with the partner requirements, the partner may move to a competitor who will comply with their preferences.

B2B relationships are already tough to keep up with and keep track of. Enterprises keep up with regulations, and now must also consider requirements coming from customers and partners which add to the complexity.

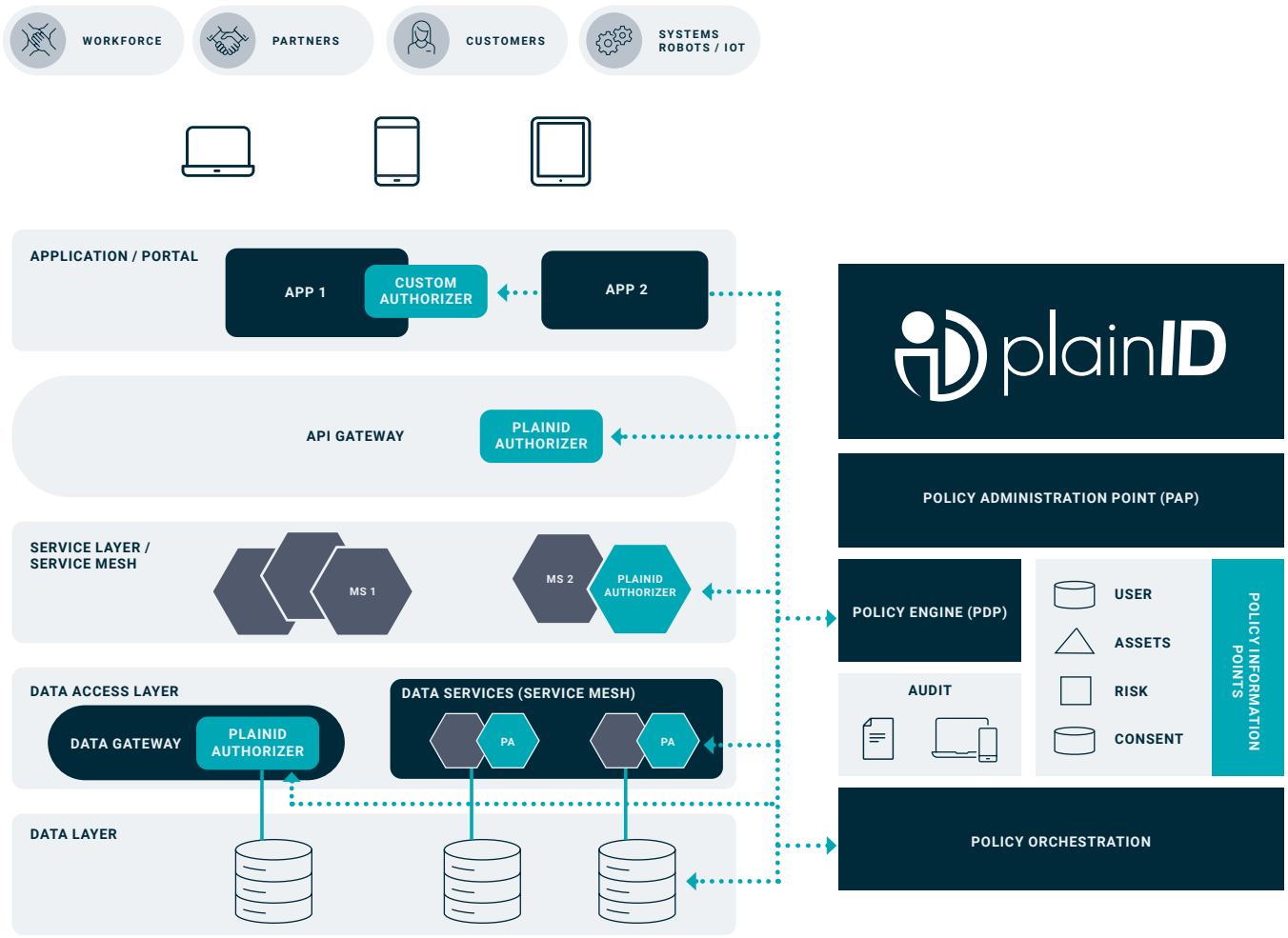
A PBAC strategy allows for B2B relationships to define their own policies. Anyone can understand and build access policies using natural language. With PBAC, enterprises can expose policy building interfaces to their third-party partners and empower them with the ability to build policies that are enforceable within their policy framework. If a certain customer partner wants their data viewable only in a specific set of countries, PBAC enables them to define the policy themselves.

With PBAC as a framework B2B customers can be in control of their own cross-border policies and its management. An Identity Security Posture Management (ISPM) platform based on the PBAC strategy standardizes the way all data access is enforced and controlled across an enterprise's ecosystem. This means that anyone who understands plain, natural language can control access.

B2B partners do not have to be experts on the internal workings of offerings, nor do they need to be experts in any specific technology. Controlling their own data processing requirements can be as easy as typing within the platform UI: only people in the US, Canada, and EU can process data owned by me. This moves the burden of the "how" to the ISPM platform solution and its integrations.

Conclusion

To consistently comply with ever-changing cross-border regulations from an end-to-end cyber perspective, a transformative shift is required. Enterprises are now moving away from siloed cybersecurity strategies and embracing a collaborative approach. By implementing a PBAC strategy such as one offered through the PlainID Identity Security Posture Management Platform, organizations can establish automated, policy-driven access controls — ensuring swift compliance adjustments towards evolving regulations. Through such transformative collaboration and automation, organizations are better equipped to effectively and efficiently navigate the challenges posed by cross-border regulations.



ABOUT PLAINID

PlainID is The Identity Security Company™ We help identity-centric enterprises defend themselves from adversaries who use identity-based attacks. Our Identity Security Posture Management Platform provides Identity Insights, SaaS Authorization Management, and Dynamic Authorization Services to create identity-centric security across SaaS, APIs, microservices, apps, and data powered by policy-based access control. **Visit PlainID.com for more information.**