Adobe Experience Platform

Adobe

WHITEPAPER

Building consumer trust with data governance

Table of Contents

Introduction

The relationship between consumers and brands has undergone significant shifts in the last decade. Increasingly, consumers are not perceiving their interactions with brands as buying just products and services, but rather as consuming the experiences that brands are delivering. Brands are also increasingly cognizant of this shift in mindset. The difference between a great and mediocre customer experience determines the engagement, retention and conversion rates for brands.

An essential part of providing great customer experiences is to personalize them based on the preferences and information that brands have about each individual consumer. As brands optimize their activities to offer personalized experiences, one of the biggest challenges is to build and maintain consumer trust. We define consumer trust as the confidence a consumer has on a brand to deliver on its promises and customer expectations. As privacy regulations proliferate worldwide, consumer expectations about privacy are growing, third-party cookies are becoming obsolete, and consumers are recovering legitimate control over their data, deciding who gets and who doesn't get access to their data. Only the brands that successfully foster consumer trust will maintain the privilege to collect and use consumer data to fuel customer experiences. In practice, this not only requires brands to deliver great products and services, but also to have the necessary controls to govern customer experience data throughout the data lifecycle, providing consumers with appropriate controls and transparency over their data.

> “Only the brands that successfully foster consumer trust will maintain the privilege to collect and use consumer data to fuel customer experiences.

Adobe Experience Platform helps brands to build customer trust and deliver better personalized experiences by centralizing and standardizing customer experience data and content across the enterprise, enabling an actionable, single view of the customer. Customer experience data can be enriched with intelligent capabilities and governed with robust data governance controls to use data responsibly while delivering personalized experiences. Experience Platform makes the data, content, and insights available to experience-delivery systems to act upon in real time, yielding compelling experiences at the right moment. An integral part of Experience Platform is its data governance capabilities that provide a framework for brands to confidently govern data, as they work to deliver real-time experiences through our open and extensible platform.

What is data governance?

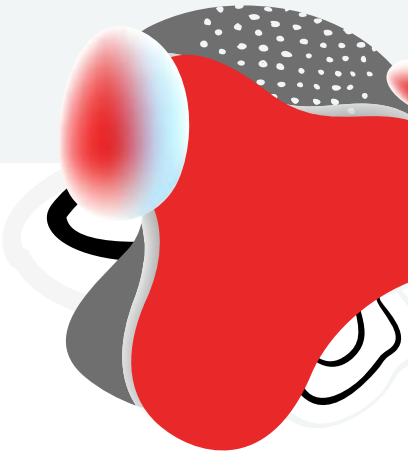
The Data Management Association International (DAMA) offers a concise definition of data governance: The exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data assets.

DAMA places data governance at the core of data management, viewing it as the discipline that serves as the foundation for all other aspects of data management.

But what does that mean to enterprises?

In the context of experience data, data governance encompasses both strategies and technologies required to deliver better customer experiences while complying with regulations, restrictions, and policies applicable to that use. It means creating a team to control data with roles and responsibilities that accommodate business needs for compliance and responsible data usage. These teams need to be supported by systems and processes that define how the various tasks for authority, control, and shared decision-making over data assets can be exercised. This means providing capabilities to enable data governance, which among other things includes data cataloging, data lineage, data usage labeling, and data usage policies.

> “Robust data governance practices and technologies enable brands to use data responsibly throughout the information lifecycle, mitigating risk of potential penalties and strengthening customer trust.



Why data governance?

Every organization today deals with data: individual bits of information about its operations, its products and services, its finances, its employees, its suppliers, distributors and competitors, and most significantly, its customers. It has become possible to not only learn a great deal about people individually and in groups, but also to create profiles of individuals that contain many dimensions of personal information. Used appropriately, these profiles can help brands to categorize individuals by various characteristics into groups, document their preferences and interests, and predict their behavior, so that brands can serve them better.

However, using customer experience data requires enterprises to comply with data usage limitations associated to that data, which may come from regulations, industry requirements and best practices, contracts and internal policies. Additionally, brands need to deliver customer experiences in a responsible manner, enabling consumers with the right controls and transparency over their data, which will foster customer trust. But this is easier said than done. The proliferation of customer data collected and used by multiple lines of business and the lack of integrated governance capabilities, makes it difficult for enterprises to make sure data is being used responsibly across the organization. Robust data governance practices and technologies enable brands to use data responsibly throughout the information lifecycle, mitigating risk of potential penalties and strengthening customer trust.

The right data governance strategy should consider the capabilities that a data-driven organization needs to succeed in today's digital world. Organizations should consider the following as they build their data governance strategy:

Adhere to rules & regulations

Understand the regulations, contractual obligations, industry requirements, and company policies that apply to experience data

Classify meta-data

Classify experience data by labeling it with appropriate meta-data

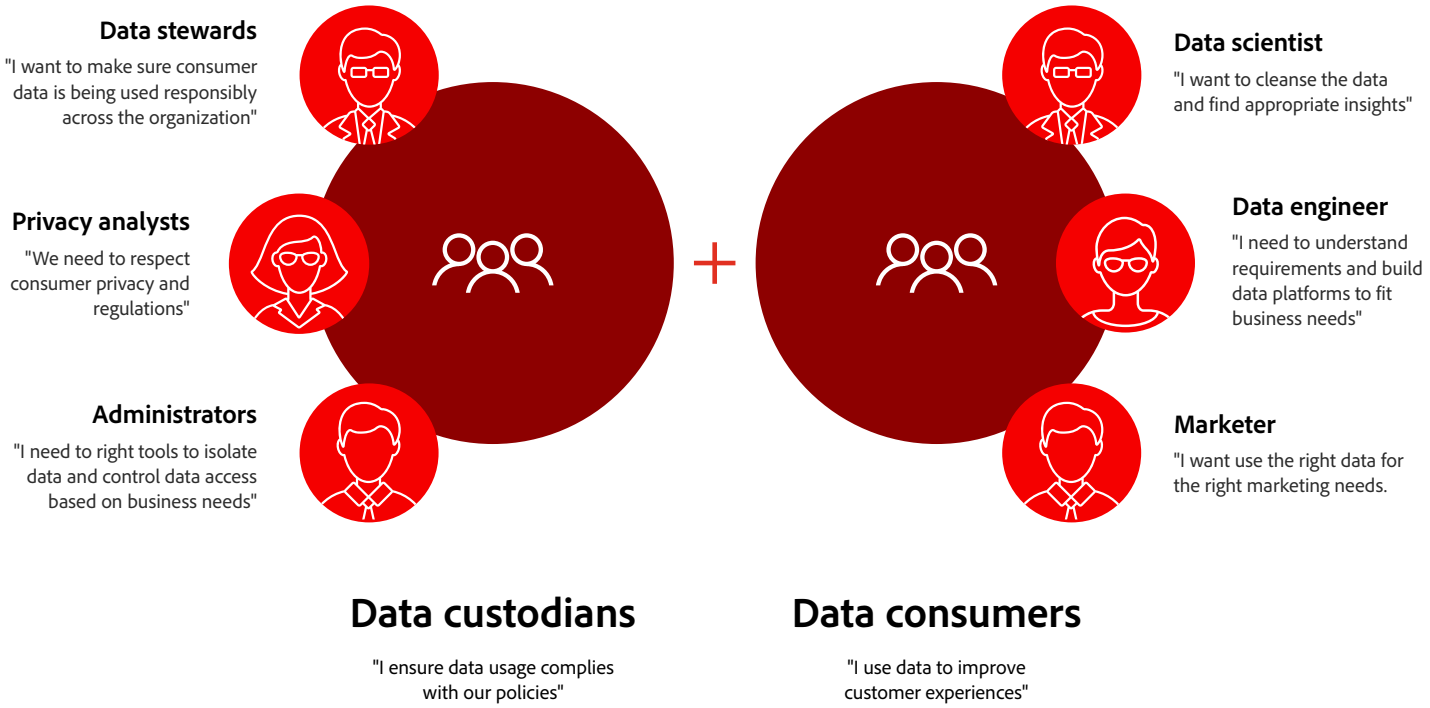
Define data policies

Define data usage policies based on various compliance, legal and corporate policies

Enforce data policies

Determine how to enforce data usage policies across the enterprise

Data governance roles



Data governance is neither automatic nor occurs in a vacuum — it is a journey involving multiple personas, which we generically classify in to two main roles: Data custodians and Data consumers.

Data custodians

At the heart of data governance, these roles are responsible for ensuring data is being used responsibly across the organization and in interactions with second and third parties. These roles may include data custodians, privacy analysts and administrators, among others, and they fulfill their obligations by:

- Interpreting regulations, contractual restrictions, and policies, and applying them to the data itself
- Applying and reviewing metadata and underlying data captured in various data assets
- Managing users access to distinct types of data and to data driven workflows

Data consumers

The end point of data governance. These are typically line of business practitioners that request data from the data governance infrastructure for different customer experience use cases. This role encompasses a number of different specialties, including the following:

- Data scientists use feature engineering workflows to enrich data and generate insights from it
- Marketing researchers make requests of data to enable them to understand customers, both individually and in groups (segments)
- Marketing specialists and Experience designers use data to design new customer experiences

Challenges to govern experience data

Putting in to practice the mandate for governing experience data in organizations is not straight forward. Inefficiencies can arise due to poor processes, undefined people roles, or legacy systems that are not well suited to meet experience data requirements. Some of the major technical challenges for data governance include the following:

1. Capabilities to manage data policies and data lineage do not integrate well with systems of engagement for customer experience. Governance solutions typically reside in systems of record and are disconnected from other systems, such as systems of engagement, preventing enterprises from automatically enforcing policy restrictions or getting visibility into the lineage of data and how data is being used by data consumers.

2. The siloed approach of managing data policies separate from systems using the data creates co-ordination inefficiencies between data custodians and data consumers in line of business. Although data custodians can set up the right policy restrictions on data and communicate it across the organization, because data could undergo multiple transformations before eventually being used by data consumers, they have poor visibility into what usage restrictions it carries and why.

3. As data consumers internalize the principles of responsible data usage, organizations need granular governance controls to balance customer's desire for privacy with their desire for relevant personalized experiences. To address this Privacy-Personalization paradox, tools need to be sophisticated enough to model complex scenarios where data usage may not be allowed for a subset of data, while allowed for certain compliant data elements.

4. Finally, the restrictions on data evolve over time as organizations change their data policies in response to regulatory and corporate needs. If the systems are rigid and cannot effectively signal incorrect data usage in response to the dynamic nature of restrictions, organizations may be blind-sided and not catch governance violations in a timely manner.

5. Every organization with presence in more than one region needs to be able to contain their data within the regulatory boundaries and business needs of that region, hence a solution for data and operational isolation is required. With that in place, customers can organize their data per region, country, brand or initiative, overcoming also any issue related to data reliability, regardless of whether data is ingested as batch or stream.

6. Organizations need to control what users, internal or external, full time or temporary, have access to what data and to what workflows are used to enrich that data. Organizations need to simplify administrators' work, enabling them to group users based on roles and responsibilities, or attributes correlated with the specifics of their functions.

The Adobe Experience Platform advantage

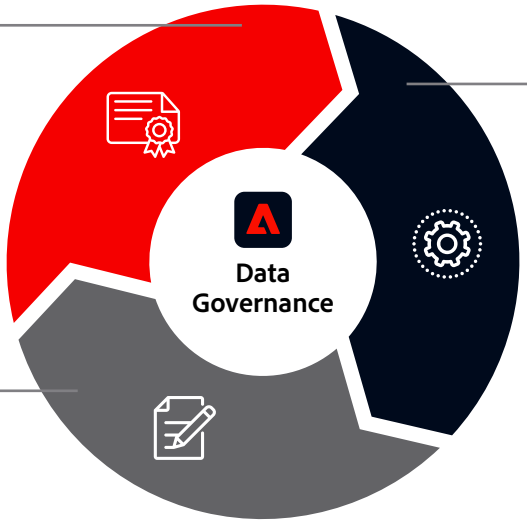
So, what's Adobe's data governance advantage? End-to-end integration. To make data governance really work, you need an integrated solution that connects your data governance infrastructure with the tools you use to create and manage customer experiences.

Patented Policy Framework

- Purpose-built for customer experience use cases
- Label data, manage and enforce policies
- Enforce policies in systems of engagement
- "Privacy by Design" in Platform workflows
- Contextual lineage to resolve policy violations

Open and Composable

- Flexibility to customize restrictions
- APIs for extensibility in custom apps
- Granularity for attribute-level restrictions



Access Control & Data Isolation

- Isolate data within the boundaries of a sandbox
- Manage user access to development and production sandboxes.
- Manage access to data and Platform workflows based on roles and policies

Adobe Experience Platform is the only solution in the market offering that kind of integration, enabling seamless controls to govern data. The governance framework on Platform provides control access to data and patented capabilities to label data, manage and enforce policies for appropriate data usage. Rich templates for common customer experience use cases are provided out of the box, encouraging brands to follow best practices and providing a framework to meet requirements for data usage restrictions.

Furthermore, all the Platform governance capabilities are built with an open and composable approach for brands to customize and use in the way they want. The API-first approach provides extensibility to integrate the features into custom applications and existing tech stacks. Adobe customers are provided with a robust set of access control capabilities that allows them to manage access to resources and workflows in Experience Platform. Data is contained withing sandboxes, providing operational and data isolation to support business and their regulatory constraints. Additionally, customization for labels and policies enables flexibility to define data usage restrictions specific to business needs.

Until now, data governance has been implemented with third-party tools on top of database platforms, and sometimes with data governance features baked into platforms themselves. But this approach doesn't provide a practical, functional data governance solution because either the tools do not have direct control over the data layer or are not flexible enough to meet the myriad of enterprise needs. By bringing governance close to the data layer in an extensible way, Platform enables brands to respond in real time to the needs of marketers and others who request use of data in the tools those professionals use - from analytics to campaign management to tools for building experiences and managing creative assets.

Data and operational isolation with sandboxes

Sandboxes in Experience Platform are the fundamental feature for data and operational isolation. Sandboxes help organizations to contain multiple initiatives, production or development focused, within their own boundaries. With sandboxes, organizations can create distinct virtual environments to safely develop and evolve digital experience applications, with full control on what sandboxes are available to specific users or groups of users. Global multi-brand organizations can capitalize on sandboxes and contain their market or brand-specific digital experience activities within the boundaries of distinct sandboxes.

Access control

Experience Platform delivers access control capabilities to provide brands with the right controls to manage their users access to the Platform workflows, data, and resources, based on their roles and business needs. These access controls help Adobe customers to address their needs with respect to data usage management, according with compliance constrains, limiting the misuse of data and leakages. At the same time, administrators benefit from a centralized administration interface where they can seamlessly manage permissions required for their users to access sandboxes and workflows such as data ingestion, data modeling, data management, profile management, identity management, and destinations.

Experience data model

Brands use multiple systems to collect and store consumer data coming from multiple sources, such as websites, third-party vendors, and offline channels. Each of these systems defines data in its own way, using different semantic definitions, virtually isolating data by system and making it difficult to govern and leverage all valuable data and derive meaningful insights across different parts of an organization. Without data standardization, data custodians cannot govern all consumer data from one place, but rather they rely on governance tools in each system, which creates data governance inconsistencies and is time consuming.

A core part of Adobe Experience Platform, Experience Data Model (XDM) is a formal specification used to represent all customer experience data in a single language or standard data model, improving data usage across the organization. For example, XDM can describe consumers' attributes and behaviors, qualify what audiences they are part of, and then categorize information about their offline interactions (such as loyalty-club memberships) and online journey (such as what buttons they click on or what they add to a shopping cart). With XDM, experience businesses can semantically normalize data coming from multiple data sources so that is equally useful and informative to sales representatives, IT departments, social media marketers, and customer service reps, allowing businesses to offer more coherent and personalized experiences in real time. Data standardization enables centralization of data governance initiatives in Experience Platform, augmenting consistency of data governance and reducing time to value for data custodians.

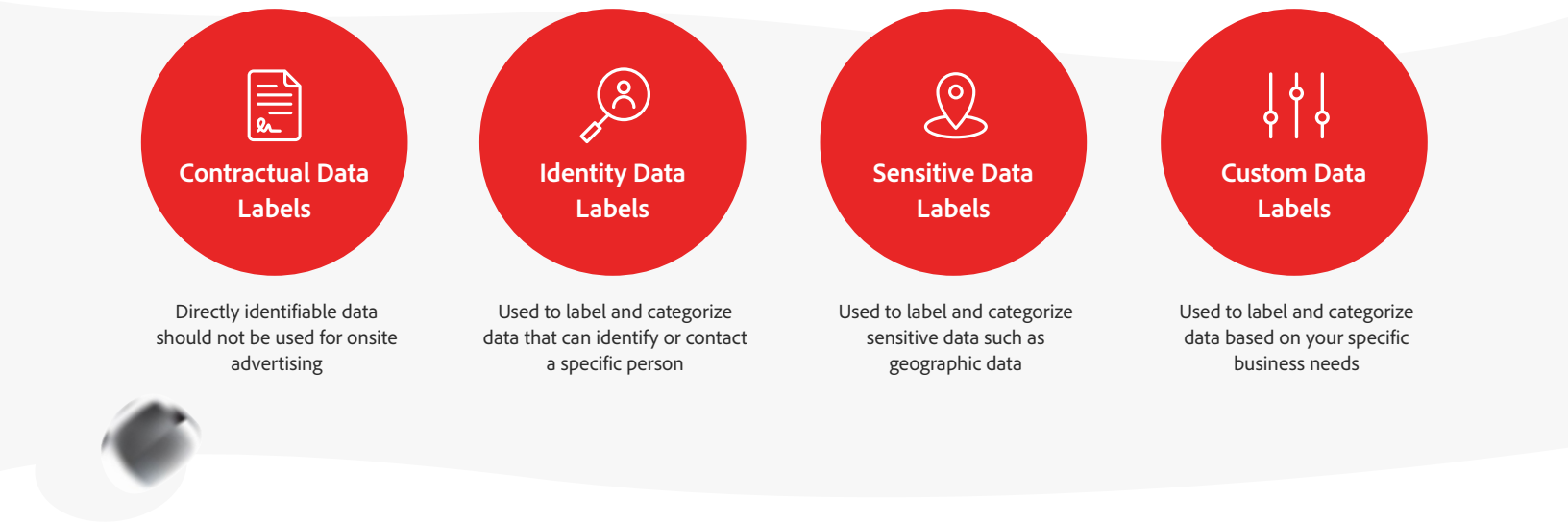
Data catalog

Adobe Experience Platform is powered by a functionally rich and easily extensible Data Catalog. All the metadata about datasets including lineage, ownership, classifications, schemas and subscriptions are maintained in the Experience Platform Data Catalog as objects. This enables users to have a single source of truth to discover and govern all data available in Platform. The metadata structure in our Data Catalog can be extended and enriched to capture additional information about specific datasets based on its purpose, source, or other characteristics. In addition to exploring datasets through Platform's UI, customers and partners can make use of the Data Catalog via APIs available through Adobe IO.

Data labeling

Adobe Experience Platform's system for classifying data starts with data usage labeling. Platform's labeling capability enables data custodians to apply classification metadata to data, either before or after data ingestion, to categorize and annotate based on governance and compliance needs. These needs could arise from the nature of the data (like personal identifiable data) or from the inherent restrictions associated with it (like data that should not be used or personalization).

Experience Platform's labeling capability includes predefined data usage labels that can be used to categorize data in three ways – contractual, identity, and sensitive. Additionally, brands can create their own custom labels to classify data based on their specific use cases and enterprise policies.



Data usage labels can be applied at dataset level for coarse-grained classifications or on individual fields within a dataset for fine-grained classifications. The framework also provides label inheritance capabilities tailored to how experience data lineage is modelled in Platform. Labels applied at the dataset level are inherited by all fields in the dataset. Labels on dataset or fields are also inherited if they are used by downstream workflows for segmentation and activation.

Data usage policies

In general, there are usage restrictions associated to consumer data that limit the way it can be used to inform customer experiences. To mitigate risks, data custodians identify these restrictions and create corporate policies that data consumers are required to comply with.

The data governance framework in Experience Platform enables data custodians to incorporate these policies in Platform, helping brands to increase visibility of data usage policies across the organization. Platform offers data usage policies templates for common experience use cases requiring data usage restrictions. Additionally, Platform includes a robust rules engine to build complex policies using Boolean expressions on the component elements, which can be extended to other systems via open APIs.

Here is how it works. Imagine a brand determines that personal identifiable information (PII) cannot be used for onsite advertising. The brand would first need to identify and label the datasets that they consider to be PII. They can use our data labels capability to catalog the appropriate data sets. Second, brands need a list of potential business actions that data consumers can use the data for. Platform provides a customer experience actions list out of the box, but brands can also customize the actions list based on their business needs. Each defined action represents a type of data use that might be requested. Typical actions may include:

Onsite personalization

Targeted email campaign

Customer segmentation

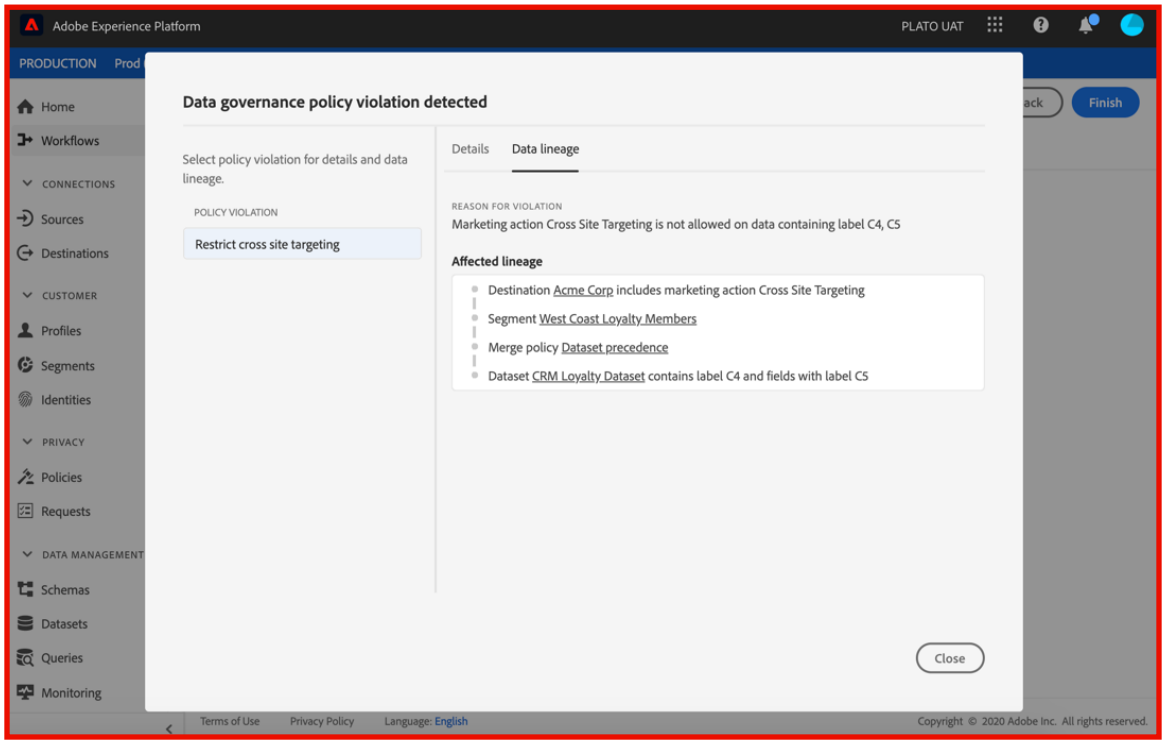
With these two building blocks in place, a data custodian can create a Boolean rule that combines the relevant data labels (PII) and the desired action (onsite advertising). In this case, if a data consumer, like a marketer, attempted to use PII for online advertising, Platform would provide guidance around why the requested use of that data is not allowed and recommend an alternative route.

Data usage policy enforcement

Once data is appropriately labelled and data usage policies are defined, Platform can enforce the policies. Data consumers using integrated applications and services can specify the purpose of the data usage and Platform automatically checks whether the intended usage violates any active policies and provides notifications accordingly. If a data consumer still wants to proceed , Platform can be configured to filter out unauthorized data and allow usage of the rest.

Platform's Governance framework embeds policy enforcement in applications native to Platform like Real-Time Customer Data Platform. Platform ensures that segmentation and activation configurations are allowed to succeed only if they do not violate any data usage policies. This ensures that data consumers are automatically restricted from non-compliant actions on Platform, such as segment definition and activation.

Furthermore, the enforcement capability also provides crucial context for why a policy violation happened. Data lineage is used to retrieve and surface the experience data relations in a way that makes sense to data consumers, so that they can understand why the action they performed is non-compliant. With this information, data consumers are not left in the dark on what they can do to be unblocked and continue their work. The lineage analysis enables data consumers to resolve policy violations by taking appropriate corrective action.



APIs for managing policies and evaluating policy violations can be used to extend policy enforcement functionality into custom applications. This enables brands to define enforcement workflows tailored to how strong are their compliance needs, including blocking data usage, surfacing warnings, providing possible remediations, etc.

Data lineage

Platform manages a comprehensive data lineage graph that tracks all the critical data relations for enforcing data usage restrictions. This lineage component is the glue that connects the policy restriction managed by data custodians with the data flow and data usage required by data consumers. Action requests are consulted with the lineage graph and validated against active policy definitions before data can be used. By taking this approach, data classifications are seamlessly propagated from source datasets to downstream data elements, like segments created by marketers. Additionally, every time a policy violation happens, the data consumer can also have access to the snapshot of the data lineage to understand why a policy was violated and get valuable context to resolve the issue.

Open governance

All Platform Governance capabilities are API-first. By leveraging our open APIs, brands can extend Platform's data governance functionality to their current tech stack for data governance. Data classifications and any purpose-based policies can be synchronized with external systems through API integrations. Additionally, policy enforcement workflows can also be integrated in custom applications that consume data from AEP using the same principles that enable enforcement on Platform.


```
{
    "name": "Export Data to Third Party",
    "status": "DRAFT",
    "marketingActionRefs": [
        "https://platform.adobe.io/data/foundation/dulepolicy/marketingActions/core/exportToThirdParty"
    ],
    "description": "Conditions under which data cannot be exported to a third party",
    "deny": {
        "operator": "AND",
        "operands": [
            {
                "label": "C1"
            },
            {
                "label": "C5"
            }
        ]
    },
    "imsOrg": "{IMS_ORG}",
    "created": 1550691551888,
    "createdClient": "{CLIENT_ID}",
    "createdUser": "{USER_ID}",
    "updated": 1550701472910,
    "updatedClient": "{CLIENT_ID}",
    "updatedUser": "{USER_ID}",
    "_links": {
        "self": {
            "href": "https://platform.adobe.io/data/foundation/dulepolicy/policies/custom/5c6dacdf685a4913dc48937c"
        }
    },
    "id": "5c6dacdf685a4913dc48937c"
}
```

Data governance in action

Data Engineer

Configures ingestion of customer data containing physical activity data

Data Stewards

Labels physical activity data

Activates policy to restrict use of such data for offsite retargeting

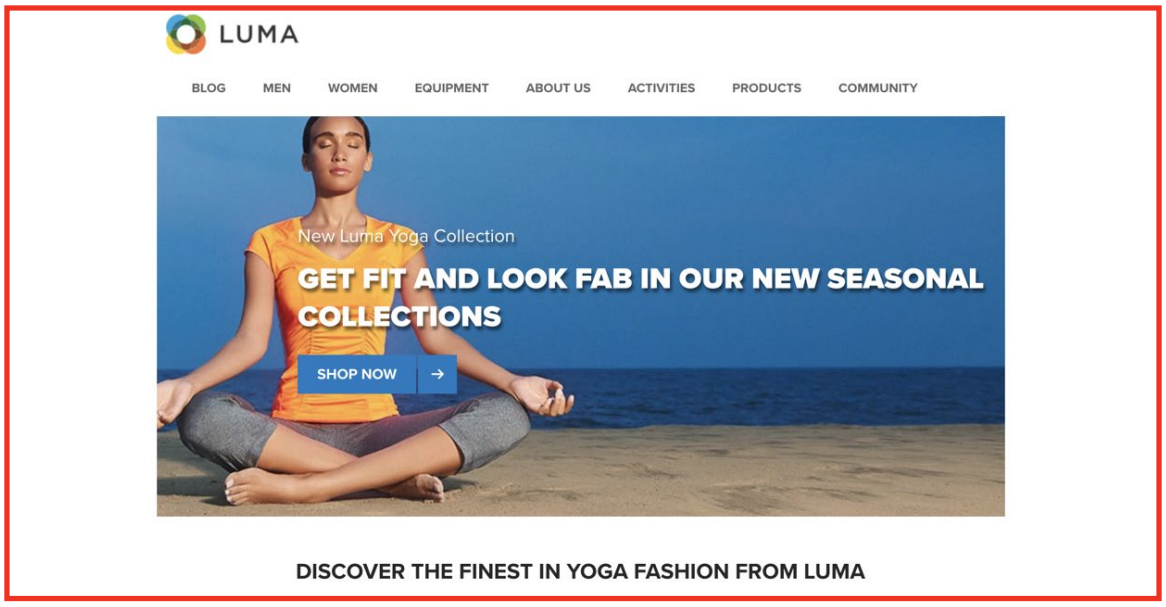
Marketer

Tries to activate a segment for offsite retargeting with physical activity data

Based on policy restriction, activation not allowed

With Adobe Experience Platform, data governance applies in real time, controlling and streamlining the process of data usage permissibility. Here's a hypothetical example on how a retailer can honor usage restrictions on its customer data in an end-to-end way using the Data Governance controls in Platform.

Luma is a growing international fitness apparel company promoting its products through several online and offline properties. Luma's CEO wants to make sure they properly manage customer data, according to applicable regulations, contractual restrictions, and data usage policies. After an intensive selection process, Luma decides to license Adobe Experience Platform in the US to enable better customer experiences while using consumer data responsibly.



With Experience Platform, Luma configures one sandbox to determine the boundaries where consumer data will be contained for their stores in the US. Then Luma clearly defines the roles that will have access to consumer data in that sandbox and the permissions for those roles. These means that Luma's administrators are able to manage their users permissions to access or edit different platform resources and workflows, as illustrated in the following link. Only specific users are granted with the permission to access resources dedicated to actions like data ingestion, data modelling, profile management, or identity management. Once these permissions are set by an administrator in Platform's administrative interface, Admin Console, every user will be able to access only specific Platform resources and workflows in line with the permissions that have been setup for them by the administrator. For more information about access controls, use this link.

With this foundational configuration in place, Luma's data custodian starts labeling data elements on Platform to indicate whether they are subject to contractual, regulatory or data usage policies restrictions and uses data catalog to create and manage data usage policies applicable across the entire organization. In this case, the data custodian uses consumer consent and preferences data to create a data usage policy to indicate that physical activity labelled data should not be used for retargeting use cases. Once the data policy is configured correctly, the Data Governance capabilities in Platform ensure that the policy restrictions are enforced.

Now Luma's data consumers can start utilizing consumer data safely. When the marketer creates a segment with physical activity data as one of its criteria, the restrictions are propagated. If this segment is used in a retargeting campaign through a social media like Facebook, policy violations are checked during the activation process and activation is not allowed due to non-compliant usage. Because of embedded governance, the marketer stays in compliance and the campaign proceeds without any lengthy data governance evaluation. This kind of efficiency is only possible when you can centralize data governance and automate usage enforcement across systems of record and engagement.

Conclusion

With Adobe Experience Platform, brands can build consumer trust by leveraging robust end-to-end data governance capabilities embedded in the very same platform they use to manage customer experiences. No other solution in the market provides this complete, seamless integration of data collection & storage, management & governance, and intelligence and real-time activation applied at an enterprise level.