Comprehensive Data Privacy Management

Global IDs Approach to GDPR
The Challenge

Customer’s expectation is their private data is protected

Regulators require that you demonstrate governance controls over private data

Data is highly distributed across an increasingly complex and interconnected data ecosystem

Securing a few high profile data silos may create a false sense of security
The Latest Data Imperative

The financial and brand impact due to non-compliance in protecting private and sensitive data is a board room issue

Today many companies struggle to comply with PCI, PHI or other PII mandates

GDPR raises the bar on privacy compliance impacting systems, processes, organizations and customer relationships

New approaches are required to bridge the world of exponential data growth, distributed data and data on demand with greater privacy compliance
GDPR A Primer

The EU General Data Protection Regulation (GDPR) will go into effect May 2018

Impacts EU and non-EU companies that process EU citizens data

Greater Enforcement

• A single enforcing agency will replace 28 regulating authorities
• Penalties as high as 20m Euros or 4% of a firm's global revenues

Greater Accountability

• 72 hour Private Data breach notification window

Greater Transparency

• Must provide visibility into how, where and why Private Data is used
• Individual consent

Data Ownership Role Reversal

• Private Data must be accessible, editable and portable by the individual
• Individual has the Right to be Forgotten
GDPR Compliance Requires Greater Transparency

What personal data is stored
Why is it being captured
Where it is stored
Where it flows
Which elements are outdated or inaccurate
Which elements must be removed
How it is protected
Transparency Simplifies Governance
Global IDs Approach to Governing Sensitive Data

Building a comprehensive Data Privacy program, as GDPR demands, is a data ecosystem problem.

Private and sensitive data comes in many formats and sources, so a heterogeneous approach is a must.

Large and complex data ecosystems require a scalable - automated approach to data discovery, profiling and organization.

Understanding the flow of data across your ecosystem is critical to assessing data source risk and remediation.

Data quality will impact an organization’s ability to meet the data transparency and change requirements of GDPR.
What Enterprise Data Management needs to do

- Create an Inventory of all data assets
- Classify each data asset based on Sensitivity
- Identify where combinations of data assets create risk
- Protect each sensitive data asset (Encryption/Pseudonymization)

  *Encryption is not the only choice for everyone or every sensitive data asset. GDPR specifically recommends Pseudonymization.*

- Put access controls on each sensitive data asset
Creating Your Inventory

The Problem
The GDPR regulation does not explicitly list a set of data elements. These must be defined on a case by case basis.
Global IDs creates the foundation for Enterprise Data Management
The Global IDs Difference

- **Ecosystem Solution**
  Designed for cross-silo data-oriented projects
  Across LOBs, countries, data centers etc.

- **Highly Scalable**
  Proven solution for ecosystems with 10,000+ databases

- **Highly Automated:**
  Uses heuristics and machine-intelligence to reduce manual effort
  Aspirational goal: 90%+ automation of data management tasks

- **Graph-Based:**
  Generates hyper-graph of data assets across the data ecosystem

- **Semantic Mapping:**
  Uses semantic concepts to map business concepts to physical databases
Summary

1. **Data Privacy is an Ecosystem Problem.**
   It cannot be solved with a silo approach

2. **GDPR Regulation is forcing the issue**
   Significant fines can be imposed for non-compliance

3. **Use scalable, automated, continuous monitoring solutions**
   A machine-centric methodology offers the most efficient approach
Thank You!

CONTACT US
+(1) 609-683-1066
info@globalids.com
www.globalids.com