perforce Delphix

2026 State of AI and Data Privacy Report

See how 500+ enterprises balance the scales between innovation and compliance.

Enterprise leaders are racing to scale their agentic development, yet the safeguards protecting sensitive data are quietly bending under that pressure. The Perforce Delphix 2026 State of AI and Data Privacy Report found that confidence in data privacy is widespread, but so are compliance exceptions, audit concerns, and data leak risks. The freight train is moving fast, and too few leaders are checking the brakes.

This report, based on responses from 518 global enterprises, shows you where data privacy mandates break down and what challenges slow AI progress. Get research-backed insights and see how your confidence can match your controls.

Key Findings

Overconfidence in Data Privacy Practices for AI/ML Environments

- 80% of organizations will invest in AI/ML data privacy in 2026–2027.
- Our respondents shared their outlook on data privacy and AI/ML:
  - 80% are highly confident in their ability to identify all their sensitive data.
  - 98% are confident in their ability to protect sensitive data in AI/ML.
  - 97% say that they're moderately to extremely confident in their ability to identify every instance of sensitive data in non-production environments.
- However, while 86% have a data privacy mandate, 84% also make data compliance exceptions.

98%

are confident in their ability to protect sensitive data in AI/ML.

How Enterprises Data Privacy Put Data at Risk in AI/ML Environments

The top 3 concerns involving AI/ML development and training environments are:

68%	62%	51%
Data leakage	Theft or breach of model training data	Unauthorized data access

But enterprises face challenges in trying to achieve data privacy in AI/ML and analytics workflows:

- 32% say it's hard to protect unstructured data sources.
- 26% say protecting data prohibits getting production-quality data.
- 25% say protecting data does not preserve relationships across data entities.

Identifying the Right Solutions That Future-Proof Data for AI/ML

- Surveyed enterprises named static data masking the top data protection approach across multiple use cases:
  - 45% chose it for software development and testing.
  - 32% for data analytics workflows.
  - 30% for integration and unit testing.
- 77% of enterprises have used synthetic data in some capacity.
  - 56% of enterprises say synthetic data is the most purpose-fit to protect data for AI/ML workflows.
  - But when paired with masking, the two together can ensure you have high-quality data for all your use cases.
- Instead of choosing between compliance and innovation, you can get trusted, compliant data where you need it using an AI-ready, enterprise solution.

Synthetic data is seen as the **#1** most purpose-fit solution to protect data for AI/ML workflows.

Be Ready as AI/ML Workflows Advance

You've heard a few insights from the 2026 State of AI and Data Privacy Report, but there's more knowledge and research to leverage. Learn about the biggest risks and how to solve them.

Get the Full Report ▶

perforce.com/resources/pdx/state-of-ai-and-data-privacy-report

Prepare for Future AI Workflows

You don't need to use point tools to get trusted, compliant data. You can get everything — masked data, synthetic data, data delivery, and governance — all in one platform with Perforce Delphix.

Built for enterprise scale and complexity, Delphix enables teams to access trusted data on demand and readies them for future agentic development to come.

Discover More About Our Data Platform ▶

perforce.com/products/delphix