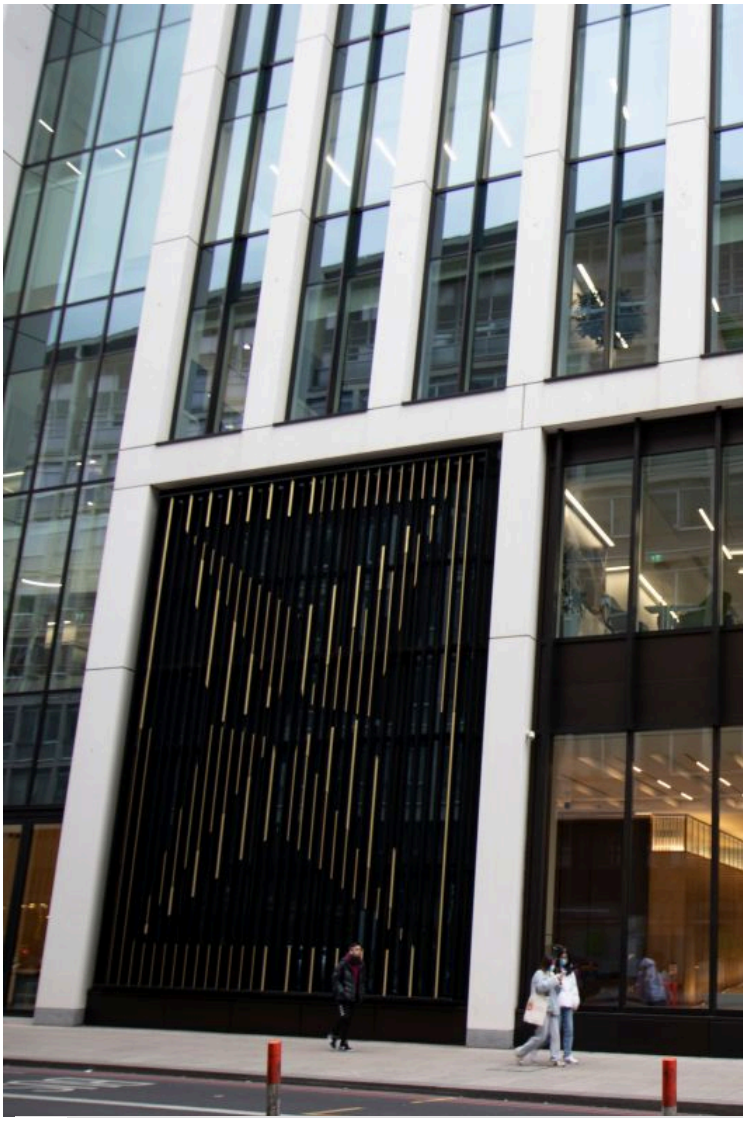
Building trust in AI

The IBM Office of Privacy and Responsible Technology help
simplify and automate global privacy and AI compliance ta
machine learning models managed by IBM



usiness Challenge Transformation Outcomes About the IBM

AI is already being used to inform decisions on whether someone should
Whether they should be granted credit or qualify for housing. It's having r
altering impacts, making it critically important that we handle AI responsi

That responsible management, however, is more easily said than done. A
Montgomery, Chief Privacy and Trust Officer at IBM, is someone who focu
AI a positive force for change.

“Within IBM, we created an AI Ethics Board—that I currently co-chair—to
challenge,” notes Montgomery. “We’ve articulated principles around AI—t
transparent and explainable. That it should be privacy preserving, secure,
fair. And while the board has helped build these principles into our culture
than faith to ensure that we’re holding ourselves accountable to them as

Fortunately, IBM had accommodated a large influx of regulations like this

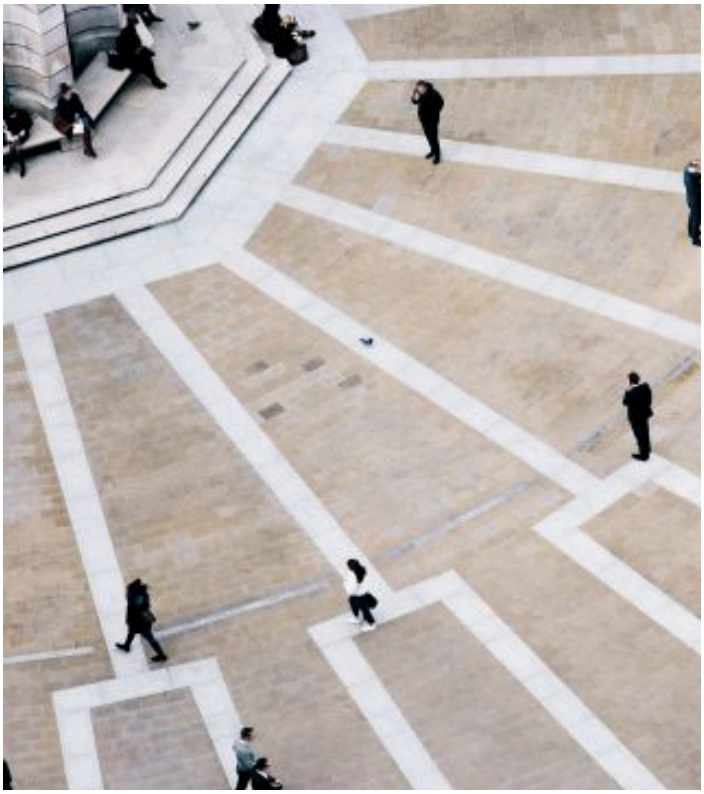
“Our GDPR [General Data Protection Regulation] compliance is probably t
analog to what we’ve had to deal with for AI,” adds Lee Cox, Vice Presider
Governance, Services, and Research within the IBM Office of Privacy and
Technology. “Prior to that, how we handled data protection-related comp
challenges was more local—many of our programs were regionalized. The
done, but we would have needed to put a fair amount of work in to scale t
new demands.”

He continues: “But with GDPR and other privacy regulations, we needed t
coordinating on a global level. We needed to adapt quickly as we faced m
more obligations, more complexity, more sensitivity about, ‘What’s happe
and how is it being consumed?’”

To handle this global oversight, IBM created an enterprise-wide Privacy a
Management System (PIMS). And based on its successes, Montgomery ar
that IBM could augment this tool to better document and track complianc
operations as well.

Much like with privacy, AI had witnessed an avalanche of new regulations
national and regional level—over the previous few years. Similarly, various
alliances and associations had also developed guidelines intended to help
behaving ethically and responsibly. But meeting this growing list of expec
hard to achieve at scale.

“We’re a big company,” adds Montgomery. “We operate in 170-plus coun
world. We consist of over 400 distinct legal entities that do business with
suppliers and 150,000 business partners. At this size, it can be difficult fr
governance perspective to get all of our more than 250,000 employees o
page.”



>5,500

applications and processes managed with PIMS

“We’ve articulated principl
should be transparent and
should be privacy preserv
and fair.”

Christina Montgomery
Chief Privacy and Trust Officer
IBM

Automate. Centralize. Contr

In late 2022, the office upgraded PIMS, now powered by IBM® OpenPages Knowledge Catalog technology. The solution, which also features innovati from the IBM Data and AI portfolio (outlined below), offers a centralized, platform able to capture, integrate and make transparent the metadata re privacy and the entire AI lifecycle, from design to deployment to everyday

"With PIMS, our overarching drivers were to standardize, simplify and sca recalls Cox. "And now we take a more continuous compliance approach th identify the gaps between what we're doing today and new regulations as out."

"It's critical that we build trust across the entire ecosystem—our employe governments and policymakers," adds Montgomery. "Which is why we're proponents of being transparent in terms of our involvement with AI, and essentially what PIMS is helping to provide."

"Bias is particularly important to consider," notes Cox. "If you take the flaws of humans and amplify that at scale through AI, those flaws are replicated across multiple systems, making the impact on society much more significant."

IBM OpenPages serves as the heart of PIMS, providing an automated, centralized workflow to previously siloed governance, risk and compliance (GRC) functions. And IBM Knowledge Catalog delivers the corresponding data catalog to monitor and curate this GRC information along with relevant knowledge assets and relationships.

As part of the IBM AI governance strategy, PIMS also takes advantage of the IBM AI Factsheets feature of IBM Cloud Pak® for Data. This tool tracks the lifecycle of machine learning models from training to production, capturing real-world data that can be used to monitor risks and model drift.

> “[N]ow we take a more continuous compliance approach that can help identify the gaps between what we’re doing today and new regulations as they come out.”

Lee Cox
Vice President of Integrated Governance, Services, and Research
IBM

In more detail

PIMS registers new instances of AI that are put into production by IBM and instances of other algorithmic systems. PIMS adds them to a centralized, company-wide workflow and assess them for potential risks. And once the model is live, the solution provides ongoing monitoring for fairness, quality and drift.

At the same time, as new regulations are passed, PIMS can be used to import these requirements, updating governance models and overall risk assessment efforts.

“There is a plethora of new AI regulations being proposed every year,” notes Cox. “It seems like every US state is in the process of building their own rules. There’s a major signature law coming out of Europe in 2024.”

With this evolving AI regulatory landscape and a continuing responsibility to maintain compliance in data privacy and data governance, IBM created an Integrated Governance Program (IGP). This IGP initiative offers a unified strategy for addressing privacy, AI or algorithmic systems, tech ethics use cases, and data clearance requests—all in the same overarching governance program, which includes PIMS.

The IGP helps IBM manage its compliance program at scale, and this will include the European Union Artificial Intelligence Act—the world’s first comprehensive AI law—which will be adopted in 2024. With IGP, AI can be aligned with the Act’s requirements, which focus on risk, trust, security and transparency, and are expected to drive new levels of human oversight and regulatory compliance for AI both within the EU and across the globe.

In turn, PIMS and associated integrated governance workflows provide increased traceability and reporting capabilities, enabling data clearance reviews to be completed before the data is used for model pretraining, development or fine-tuning. The tool also helps to maintain accurate documentation and records of processing (RoPs), associated training, testing metrics and current predictions—regarding AI and other algorithmic systems. Similarly, IBM staff can use this document trail to verify that remediations are actually completed.

IBM plans for future versions of PIMS to reflect IBM’s latest watsonx™ product suite, including watsonx.governance™. This move is intended to provide IBM with enhanced model lifecycle governance capabilities, key metrics and broader performance benchmarking reports.

"[W]e can offer a level of transparency that can help our partners and clients build the confidence, the trust that project by project they can adopt this AI technology while managing—keeping an eye on—risk."

Christina Montgomery
Chief Privacy and Trust Officer
IBM

More compliance, less work

Presently, PIMS is tracking and managing over 5,500 enterprise applications and business processes across global IBM operations—all from a single, unified platform. And the automation features delivered by the tool feed relevant key performance indicators (KPIs) to governance dashboards, designed to help simplify management, cut overhead, lower remediation workloads and accelerate speed to compliance.

“Rather than having every asset, every individual, every application, every business process monitored by the process owner—and forcing them to work out what laws need to be complied with—we mask that complexity,” explains Cox. “With PIMS, now they only have to focus on the automatically generated remediation tasks. That translates to thousands of hours of effort saved across all of IBM.”

And as new regulations roll out, IBM can identify and accommodate their requirements much more quickly.

“Our last big project—GDPR—took about 12 months of effort to put in a governance model and tracking solution,” notes Cox. “With PIMS, we can now launch an enterprise-wide regulatory compliance program in greatly reduced times, sometimes as short as six weeks. The information’s already there, which makes it faster and easier to identify gaps and build the campaign. After launch, PIMS can then feed the relevant tracking and remediation data automatically into our dashboards.”

And this speed is critical when accommodating new rules. As Montgomery explains: “When a major regulation is enacted, it’s often unlikely that we’re going to be given a ramp-up time of two to three years. It could be more like four to five months. And if our partners or clients don’t have PIMS or something similar to rely on—tools that deliver always-on inventory management and a robust understanding of what data is used throughout the enterprise—then they are going to struggle with compliance.”

“But when they work with IBM,” she continues, “we can offer a level of transparency that can help our partners and clients build the confidence, the trust that project by project they can adopt this AI technology while managing—keeping an eye on—risk.”

About the IBM Office of Privacy and Responsible Technology

The IBM Office of Privacy and Responsible Technology oversees the creation and administration of global IBM policies regarding the protection and confidentiality of individual and business data. And working in conjunction with the IBM AI Ethics Board, the office guides the governance and relevant decision-making processes for AI ethics policies and practices, building a culture of responsibility and trust throughout IBM.

Solution components

- IBM Cloud Pak® for Data →
- IBM® Knowledge Catalog →
- IBM OpenPages® →
- IBM watsonx.governance™ →

Make AI do what you want

Manage the oversight, direction and governance of your AI activities with IBM watsonx.governance technology.

Explore IBM watsonx.governance →

Explore our AI Governance Services →

results will depend entirely on the client's systems and services ordered. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.