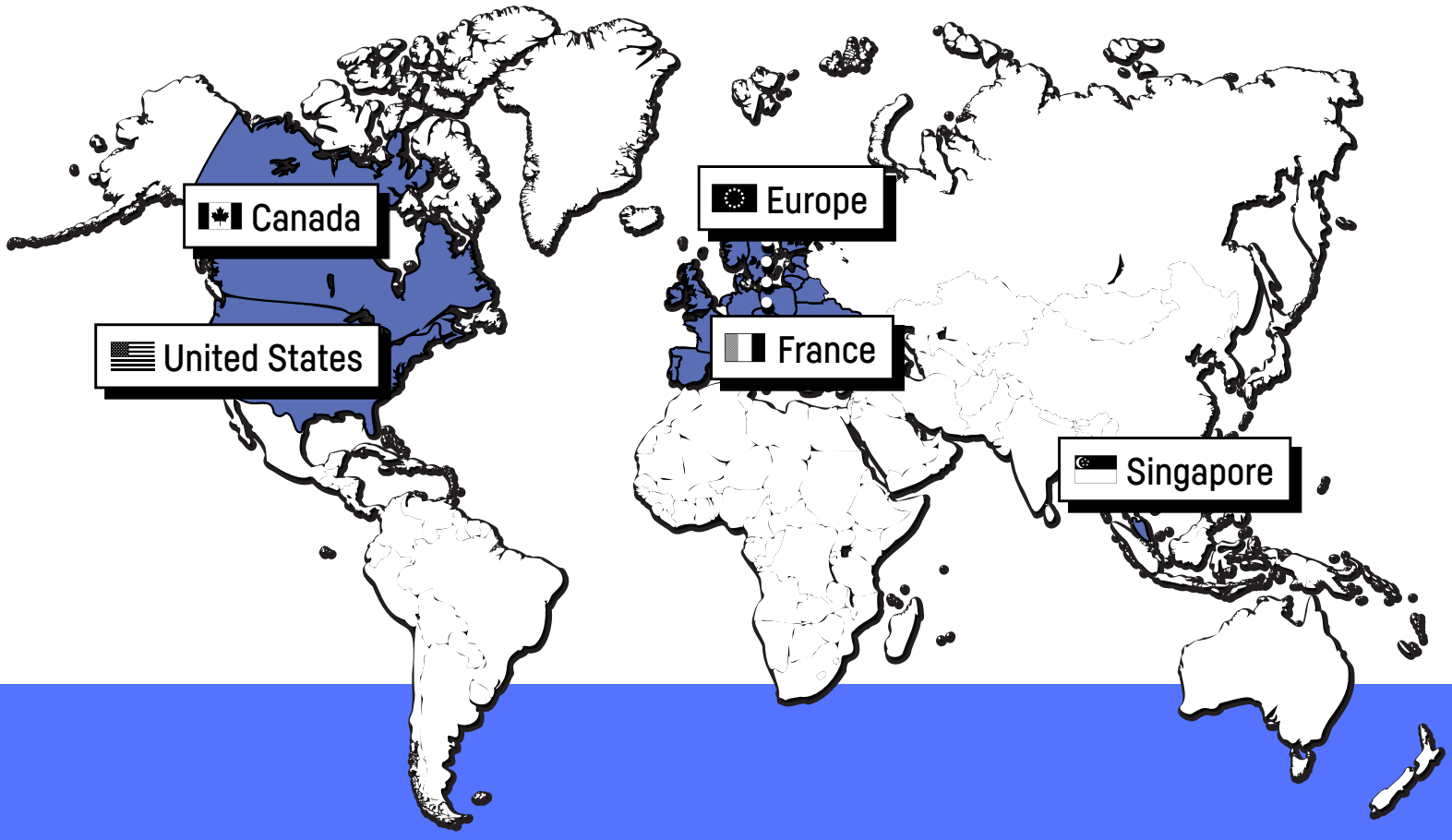
data iku

EBOOK

A Global Look at Emerging Regulatory Frameworks for AI Governance

Table of Contents



Click on a specific location to
jump to that section of the ebook!

Introduction

Let's get right into it — without understanding the concept of AI Governance and the reality of upcoming regulations (and their impact), scaling analytics and AI as a way to maximize business impact is not feasible. As organizations wish to scale with AI by multiplying (and usually complexifying) the number of projects moving to production, they face new challenges:

1. **Inefficiency**

   A rapidly growing stack of projects requires managing more people, more processes, and more technology. While AI talent is scarce, the technology stack is ever expanding and the process to manage it creates inefficiency. Pushing a project to production shouldn't take months but hours.

2. **Production Risks**

   Pushing projects into production involves a new set of risks that are very different from development. Data protection, opacity, or biases become tangible issues that can harm an organization's reputation and financial performance.

3. **Legal Pressure**

   Production risks have been identified and discussed by regulators around the world for the last few years. Today, a growing number are proposing regulations to set new standards for AI Governance for the private sector, with potential fines for non-compliance.

Making the move towards Everyday AI, or systemizing the use of data and AI for better day-to-day decisions, requires organizations to invest in the right governance to address these challenges before it's too late.

So, you're probably wondering why it's important to think about the topic of AI Governance with a global perspective (which, as you'll see, is how this ebook is organized). First, to take the example of the Artificial Intelligence Act, even though it is a European regulation, companies that operate or have customers in Europe still need to adhere to its requirements. This means it's possible that, even if you're a U.S.-based company, you will have to follow European AI regulations.

Secondly, a key takeaway from writing this ebook is the observation that each regulation and guidance tends to be viewed in a siloed way. Maintaining a pulse on how different geographic regions handle AI Governance and regulatory compliance is a good litmus test of what's to come — certain countries are further along than others so the global view helps give a diversified perspective of emerging global patterns when it comes to AI regulation (and equips each geo with key resources to leverage).

What AI Governance Means and How AI Regulations Fit In

Before we deep dive into the upcoming AI regulations, here's the best way to think about AI Governance and its link with AI regulation. When it comes to AI, governance is a framework (enabling processes, policies, and internal enforcement) that ties together operational (MLOps) and values-based (Responsible AI) requirements to enforce consistent and repeatable processes aimed at efficiently delivering AI at scale. More specifically, it helps manage operational risks and maintain legal compliance for AI and advanced analytics projects.

In other words, AI regulation is one piece of the AI Governance puzzle. AI Governance delivers end-to-end project and model management at scale, with a focus on risk-adjusted value delivery and efficiency in AI scaling, in alignment with upcoming regulations. At Dataiku, we look at AI Governance as an opportunity to build resilience by developing an operational model to:

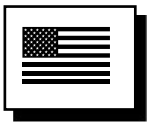
Support accelerated AI growth.

Eliminate silos between teams.

Foster alignment and oversight transversally.

Dataiku enables users to view the projects, models, and resources that are being used and how. The full range of documentation capabilities (e.g., audit trails, model documentation generator, fairness reports) enable organizations to streamline the production of necessary auditing material. The capacity to easily organize audits and reviews of existing models and leverage a broad set of explainability and fairness tools supports fully intentional and controlled AI development.

This ebook highlights emerging regulatory frameworks that are on pace to deeply reshape how AI is scaled. These proposed directives, regulations, and guidelines provide helpful learnings and best practices (across Europe, North America, and southeast Asia) for AI and analytics leads who are keen to be able to react accordingly and scale their data science and AI efforts in a way that is responsible, in line with regulatory compliance, and sustainable for the future.



Zooming in on the U.S.

In this section, we're focusing on not one but a couple of ongoing legislative initiatives unfolding in the United States. We will be taking a bird's eye view to learn about the shifting dynamics of one of the countries that has so far privileged AI self-regulation over regulation.

Why? Since the EU's AI Regulation proposal, which called for a ban on specific types of AI applications and tight governance of others, there has been a lot of discussion about the implications of such a proposal on countries that haven't taken much of a stance yet. The U.S. is one of them and it seems like the Wild West days of AI are counted!

The Wild West of AI

In 2016, the U.S. government was one of the first to draw attention to the questions that progress in AI raises for society. Many guidelines, outlining principles, and recommendations followed from various government offices (i.e., The White House's Office of Science and Technology Policy[1], the National Institute of Standards and Technology[2], and the Department of Defense Innovation Board[3], to name a few) but the motion hit a wall: regulation should be avoided where it "needlessly hamper[s] AI innovation and growth." In 2020, the administration called for further deregulation.[4]

Interestingly enough, the reaction of many companies was not to go ungoverned in the absence of a legal framework. We have notably seen many technology players establish their own ethical principles charter[5] or dedicated governance committee[6] as a way to organize their efforts and identify dos and don'ts.

The days of self-regulation are now long gone. As companies increasingly deploy their solutions on the market and AI scandals are continuously echoed throughout the media, a framework to systematically analyze AI systems' risk seems fundamental — especially when the solutions deployed affect all walks of life, nearly everywhere, at any time.[7]

[1] *https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf*
[2] *https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf*
[3] *https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF*
[4] *https://www.federalregister.gov/documents/2020/01/13/2020-00261/request-for-comments-on-a-draft-memorandum-to-the-heads-of-executive-departments-and-agencies*
[5] *https://ai.google/principles/*
[6] *https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1:primaryr5*
[7] *https://www.ft.com/content/e082b01d-fbd6-4ea5-a0d2-05bc5ad7176c*

In a timely manner, the National Security Commission for Artificial Intelligence's March 2021 Final Report[8] urged the adoption of a cohesive and comprehensive federal AI strategy. But what should this strategy look like for policymakers facing historical pushback on regulation?

The Wild West Isn't so Wild Anymore

The answer might lie in a series of initiatives that is adding pressure on policymakers.

Throughout the years, at the federal level, there was only one proposed legislation that was attempting to swim against the tide. Introduced in 2019 in Congress, by Senator Wyden of Oregon, the Algorithmic Accountability Act (AAA)[9], intended to make impact assessment a requirement for organizations using their software for sensitive automated decisions or to "make decisions that can change lives." The bill would have been overseen by the Federal Trade Commission (FTC) and would have applied to both new and existing systems. This bill never progressed past committee level.

[8] *https://reports.nscai.gov/final-report/table-of-contents/*
[9] *https://www.wyden.senate.gov/news/press-releases/wyden-booker-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms-*

Yet, with the new political landscape, and the growth in national frameworks — with the EU at the forefront — the bill could come back into fashion. It is planned to be reintroduced in the future[10] and is likely to benefit from much stronger momentum:

1. The bill echoes popular requests for end-customer protection.

The AAA bill would require companies to assess their use of AI systems, including training data, for impacts on accuracy, fairness, bias, discrimination, privacy, and security, with the ultimate objective of better protecting end customers. Strong reactions to recent controversies have shown how important it is to U.S. citizens. The fact that these criteria and more are articulated in the European proposal might bring additional legitimacy to the new AAA bill.

2. The bill leverages a federal agency that has its own agenda.

The bill entrusted the FTC to oversee its implementation, and rightly so! In a short blog post last April,[11] the FTC outlined that it plans to go after companies using and selling biased algorithms. It also plans to verify claims about AI products that would not be "truthful, non-deceptive, and backed up by evidence." Although it might take many legal challenges in court to make this a standard, it's a very good start.

3. The regulatory environment for key sectors, alike pharmaceutical and financial services, is reaching maturity.

Industry-specific agencies, like the FDA (Food and Drug Administration) or the FED (Federal Reserve System) have been implementing requirements (GxP for life science organizations and SR 11-7 for financial services organizations[12]) to ensure safety for sold products and services. As these organizations modernize and leverage AI, they need to match these requirements too. In other words, AI regulation might build on existing regulations which are already applicable to AI systems in specific industries.

[10] *https://www.meritalk.com/articles/sen-wyden-to-reintroduce-ai-bias-bill-in-coming-months/*
[11] *https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai*
[12] *https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf*

4. The new administration is committed to modernize.

President Biden's initial economic recovery plan[13] included a $9 billion increase to the Technology Modernization Fund (TMF), along with other funding measures to upgrade federal government technology and improve IT security. Although the TMF funding was cut[14], it showed a clear direction for the new administration on IT modernization. Such direction materialized in the launch of the National Artificial Intelligence Research Resource Task Force that aims to promote access to research tools for AI and the National AI Advisory Committee which provides recommendations and advice on AI topics, including economic competitiveness and societal, ethical, legal, safety, and security matters.[15]

5. New actors are feeling increasingly comfortable with tackling algorithmic discrimination.

Lawyers are updating their tools for the algorithmic age. Whether it is for housing discrimination[16], credit[17], or any fundamental services (similarly to the EU proposal by the way), lawsuits are creating precedent and are expanding customer rights.

[13] https://www.meritalk.com/articles/biden-plan-tmf/
[14] https://www.meritalk.com/articles/tmf-funding-boost-dropped-from-1-9-trillion-relief-bill/
[15] https://www.whitehouse.gov/ostp/news-updates/2021/06/10/the-biden-administration-launches-the-national-artificial-intelligence-research-resource-task-force/
[16] https://www.washingtonpost.com/business/2020/11/02/housing-groups-sue-redfin-alleging-federal-discrimination-violations/
[17] https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/
[18] https://www.wired.com/story/new-york-city-proposes-regulating-algorithms-hiring/

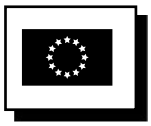
On the other hand, cities like New York are also proposing laws to regulate AI[18]. In this case, the New York City Council wishes to update hiring discrimination rules to cover AI software. Similarly to the AAA, companies would be required to perform annual audits to ensure their technology is not discriminatory.

Indirectly, these elements will influence the upcoming AI regulation debate that is waiting to happen (see existing measures across the U.S. to consider AI's impacts[19]). It's highly likely that in two years AI policy tools, whether binding or not, will be effective and enforced. Then, it might be too late for organizations that didn't anticipate governance and compliance requirements.

Do You Have the Right Ammunition in Your Toolbox?

It's hard to deny it — AI will need to rhyme with governance and compliance very soon. Our advice is simple: don't wait! If you do, it's likely that your organization will create some AI Governance debt (i.e., the implied cost of additional rework by choosing not to address AI Governance stakes early enough in the development and commercial process). For example, you might find yourself in a "hands up!" situation when the regulator asks you "Where are your models?" or "What are the metrics you chose to validate your models?"

[19] *https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx*



Zooming in on Europe

In this section, we're focusing on the recently introduced "Artificial Intelligence Act" by the European Commission, the executive branch of the European Union (EU), responsible for proposing legislation, implementing decisions, upholding the EU treaties, and managing the day-to-day business of the EU. The European Commission is the first institution worldwide to propose a new legal framework to harmonize rules regarding AI use. This proposition will still need to go through the European Parliament and the European Council, yet it is likely to become the new gold standard for all organizations around the world building, using, and/or selling AI systems.

Here, we're going to build on the insights we have gained not only from the EU but also from France. So far, national regulators seem to have relied on existing legislation — most of the time data protection regulations — to introduce AI rule enforcement. It's a different game this time around! The European Commission (EC) is proposing a brand new regulatory framework to protect citizens from harmful AI [20]. This is a first-of-its-kind initiative that will highly shape AI development and deployment standards around the world, similar to how GDPR influenced data protection globally.[21] This proposal is likely to add pressure on other regulators to take bolder stances to govern AI.

Wait, Why is AI Regulation Needed Again?

AI is a deeply transformative technology. Through the processing of large amounts of data, AI models can automatically generate high-value content, predictions, recommendations, or decisions on a wide range of topics (i.e., targeted ads, facial recognition, self-driving cars).

Yet, as the European's proposed regulation indicates, some applications of this technology can be difficult to understand or control over time, and the data fed to AI systems can perpetuate biases and discriminations. These harms endanger the fundamental rights of EU citizens, such as non-discrimination. After three years of research and consultations, the EC is proposing a regulatory framework to the European Council and the European Parliament to address AI risks and to maximize its benefits.[22]

[20] *https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence*
[21] *https://www.cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/*
[22] *https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence*

How Will AI Be Regulated?

Upon the feedback gathered last year from their white paper, the EC has chosen a risk-based approach to regulate AI in the European market.[23] The objective of such an approach is to assess the risk of any given product or service before and after it is launched to the market to ultimately prevent harm to EU citizens.

The EC proposal defines four risk categories with more or less strict compliance procedures. The rule of thumb is "the higher the risk, the stricter the rule."

We've outlined the categories below:

Unacceptable risk
Practices identified as a clear threat are banned (i.e., social scoring, facial recognition in public spaces, extreme nudging).

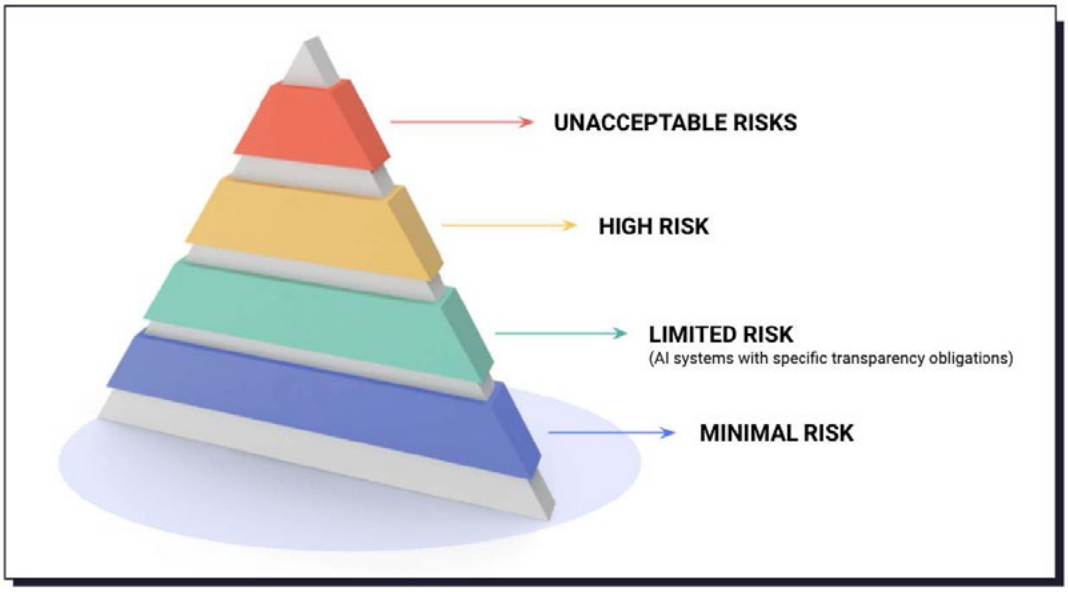
High risk
Practices identified as a potential threat will have to be demonstrated as safe (i.e., essential private and public services such as obtaining a loan, transportation infrastructure, educational training, human resources, border controls, justice administration).

Limited risk
Systems with limited threats, like chatbots, will be subjected to transparency obligations to ensure users make informed decisions (i.e. the user can then decide to continue or step back from using the application).

Minimal risk
Most AI systems fall into this category and are to be freely used.

[23] *https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence*

Military uses of AI are excluded from the above. Please refer to the EC proposal for an extended definition of targeted practices.[24]



The AI risk classification of the EC[25]

While providers and users of low-risk AI systems will be encouraged to adopt (non-legally binding) codes of conduct on use, high-risk AI systems providers and users will be required to undergo extensive reviews before products or services can be leveraged.

Go-to-market requirements include:

1. Conformity assessment to evaluate the risk of the application according to the risk classification shown above

2. Compliance with AI requirements (based on the assessment, a third party might be involved)

- Activity logging to ensure traceable results
- High dataset quality to minimize risk and discriminatory outcomes
- High levels of transparency, robustness, accuracy, and security
- Human oversight (system design and use) to minimize risk
- Overall risk management and documentation

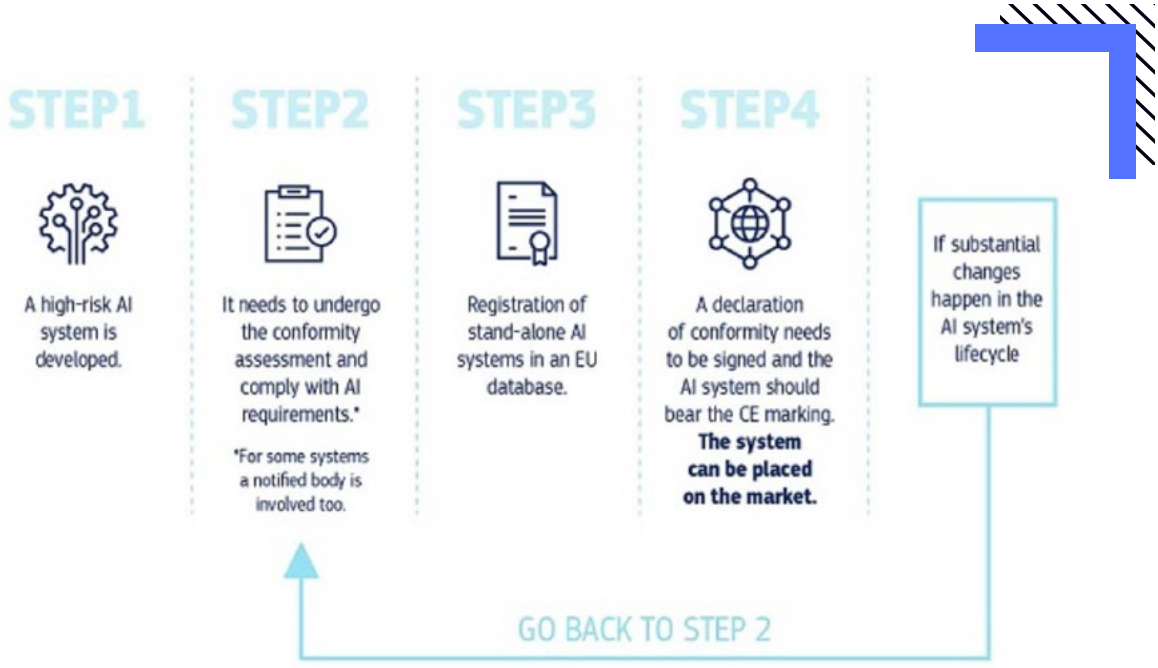
[24] *https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence*
[25] *https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence*

3. Reporting (subject to variations whether a business is providing, importing, distributing, or using the AI product or service)

- Registration of the system in an EU database
- Declaration of conformity is to be signed
- The system should bear the CE marking[26] and include:
  - Clear and adequate user information
  - Detailed technical documentation for compliance checks

4. If substantial changes happen in the system's lifecycle, a new conformity assessment must be conducted

Providers are also specifically responsible to report any major incident with a given system once it is commercialized. Not complying with the high-risk requirements would open the possibility of a 4% global annual revenue fee (capped at 20 million euros) and a 6% global annual revenue fee (capped at 30 million euros) in case of the banned AI practices (described above).



Rules for providers of high-risk AI systems [27]

[26] *https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm*
[27] *https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence*

Who Will Be Impacted by the AI Regulation?

Any user of AI systems in the EU

Any company selling AI products or services in the EU, whether or not they are based in the EU

Any providers and users of AI systems that are located in a non-EU country but where the output produced by the system is used in the EU

How Will This Proposal Be Enforced?

The EC proposes a coordinated plan to ensure the implementation of the proposal once it is validated by the European Parliament and the European Council:

All member states will put the regulation into practice by enacting their own laws. National regulators will be selected to interpret the European law for the national scope.

The EC will oversee the coordination with member states and the high-risk system register while the European Artificial Intelligence Board (EAIB), a new supervisory authority suggested in the proposal, would oversee the enforcement (including post-market surveillance).

The regulation would first enter into force in the second half of 2022 to develop standards and governance structures before being fully implemented during the second half of 2024.

What Does This Framework Mean for Organizations Scaling AI?

Actually a lot! If binding regulation seems inevitable for the European market, what are the upcoming opportunities and roadblocks for organizations? Here are some insights to support your planning:

1. There are a lot of governance resources already available from national regulators.
Indeed, they have been working for the last few years on the potential risks of AI and gone through extensive research and stakeholder consultations. See for example the work of the French Financial Services regulator, ACPR, later in this section.

2. These resources need to be articulated within the company to build robust processes.
Although we have observed the establishment of ethical principles or checklists during the last few years, most organizations have not yet entirely formalized or implemented their AI Governance processes. It will be key to do so before starting to work on regulatory compliance, especially since governance is an opportunity to make your development and deployment processes more efficient!

3. The processes then need to be enforced.
Identifying risks for all the AI systems across the organization and following the established processes in a consistent manner for each of them will be the main challenge. Ensuring that these efforts do not slow down AI development and its successful embedding in key business processes will be another — especially when we know how much is still to be done in this space. Having a platform approach with tier-one auditability and governance features such as the ones provided by Dataiku will be paramount to evolve in this new environment.

While the EU regulation could be seen by a few as a blocker to AI, we are convinced that it will pave the way to sound AI development, supported by strong governance principles capable of inspiring trust in AI capabilities throughout industries.

French AI Regulations

According to the European Commission proposal, France, like all other member states of the EU, will be expected to align its own national regulations on the proposal once it is validated. Therefore, while the proposal is being discussed, national and industry regulators across the European Union (like ACPR) are working on scoping these topics for their respective mandates. This scoping work highlights the shift away from general AI regulation to industry-specific approaches to AI regulation.

In June 2020, the French Financial Services Regulator (ACPR, which is responsible for ensuring financial stability and consumer protection in France) published a unique reflection document titled "Governance of Artificial Intelligence Algorithms in the Financial Sector."[28] From explainability standards to governance protocols, the 80-page document provides concrete insights into what will be asked from banking and insurance organizations operating in France in terms of compliance.

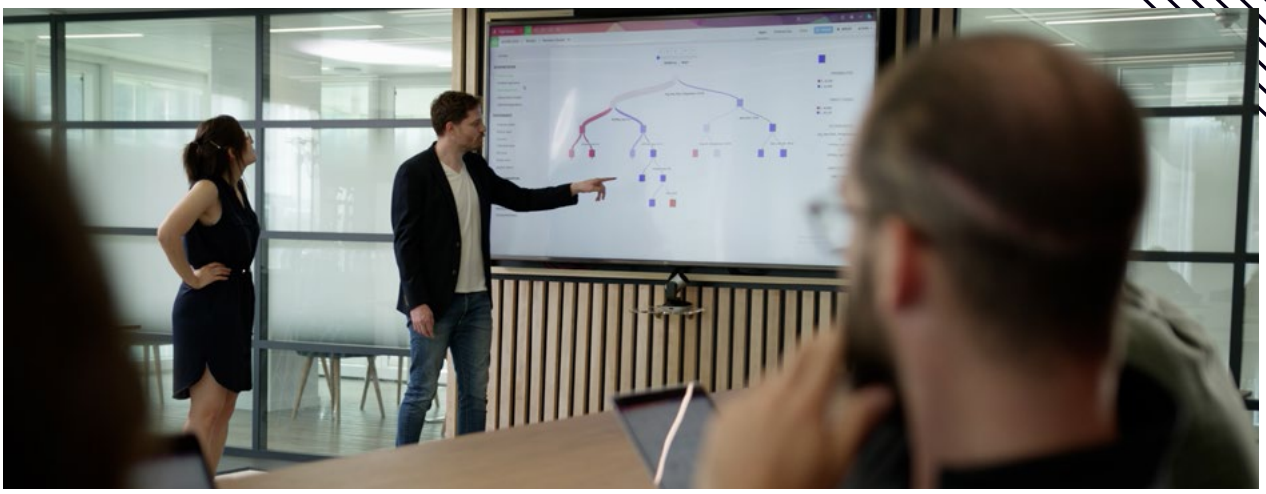
In 2021, the ACPR has been working even harder to operationalize it's own vision for explainability through a "tech sprint,"[29] gathering financial services actors to explain credit scoring predictive models. Such a format has helped many French actors test their own understanding of upcoming compliance requirements.

[28] *https://acpr.banque-france.fr/en/governance-artificial-intelligence-finance*
[29] *https://acpr.banque-france.fr/autoriser/fintech-et-innovation/tech-sprint-sur-lexplicabilite-des-algorithmes*

The ACPR Paper Suggests a Radically Different Approach to Governing AI

ACPR's publication is the result of two years of research with French financial actors and their use cases (e.g., anti-money laundering/combating the financing of terrorism, credit scoring, etc.). It is divided into two main chapters: the assessment of AI algorithms on the one hand and their governance on the other. Simply put, how can we best assess AI risks and leverage the assessment outputs to address these risks?

AI risks should no longer be understood as standalone technical anomalies but as core business issues. Governing AI risks thus requires an update to the traditional risk and compliance corporate expertise.



If you remember three things from the ACPR paper, keep in mind the ones below:

1. Companies need to build capabilities for AI regulation now by assessing and managing the risks of their AI projects.

2. AI risk assessment is the translation of core principles (e.g., explainability) into risk metrics and scores. These metrics cover not only technical elements of the AI lifecycle but also business and organizational elements.

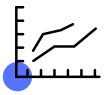
3. AI risk management or governance is using the risk assessment outputs to address the risks. Yet, before you can do that you need to have established roles and responsibilities, a risk framework, and governance protocols.

Let's Review the Assessment Piece First

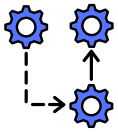
Similar to the European approaches to regulatory framework building, the paper starts by recalling that principles are fundamental to drive any assessment.

Here, the four main risk criteria listed are:

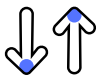
Data Management
Ensuring the quality of the data



Performance
Ensuring the quality of the model



Stability
Ensuring the consistency of the model



Explainability
Ensuring the transparency of the model and its outputs

While the first three criteria make sure the assessment is reliable, the last criterion makes sure anyone can conduct and/or understand the assessment. This is the shift between technical and business approaches to AI Governance.

That was a first key takeaway but there's more: The last risk criterion, explainability, is not a binary concept (is your model explainable or not?) but a continuous concept (i.e., to what extent is your model explainable?). Moreover, the explainability concept is dependent on external factors like the audience (e.g., explainability cannot be delivered the same way to auditors, internal controllers, or consumers) and the risk (e.g., the severity and likelihood of the risk of not explaining well is different from a risk to another). In a nutshell, explainability is not a one-size-fits-all concept and requires in-depth work to understand and successfully operationalize for business and compliance value.

Use Case			Explainability Criteria			Explainability Level Required
Domain	Business Process	AI Function	Explainability Audience	Context	Associated Risk	
Insurance Contracts	Contract Management	Proposing Compensations	Client	Compensation Process	Operational Risk (unsatisfied client)	1
			Internal Controller	Daily Process Control	-Operational Risk -Conformity Risk -Financial Risk	2
			Auditor	Algorithm Assessment	-Operational Risk -Conformity Risk -Financial Risk	3
	Sales Offering	Prefilling Quotations	Client	Asking Quotations Online	Conformity Risk (wrong client information, advisory duty, discriminatory biases)	3
			Internal Controller or Auditor	Conformity Assessment	Conformity Risk (wrong client information, advisory duty, discriminatory biases)	3

Figure 1. Table from the ACPR paper listing the different levels of explainability for the key external factors (i.e., the audience and the business risk). The translation to English was done by Dataiku.

Moving Forward to the Governance Piece

Distinctively from the European approaches, the paper tries to tie the assessment to the governance in a very concrete manner to encourage organizations to start updating their risk approaches now:

First, by formalizing the roles, responsibilities, and means to carry them out. Who is responsible (and qualified) to assess AI and develop the governance protocols to address AI risks? The ACPR paper suggests it is the role of internal control, and the governance protocols should have at least three different control levels.

Second, by updating the risk framework regularly to enable a coherent and consistent view of risks across the organization. Once the risk framework has been set, the ACPR suggests building appropriate training to ensure the risk analysis is cross-cutting and updated over time.

Third, by developing and testing an audit methodology. This is a fundamental element of any future AI regulation. The ACPR suggests taking into account the development context of the algorithm as well as of the business lines impacted.

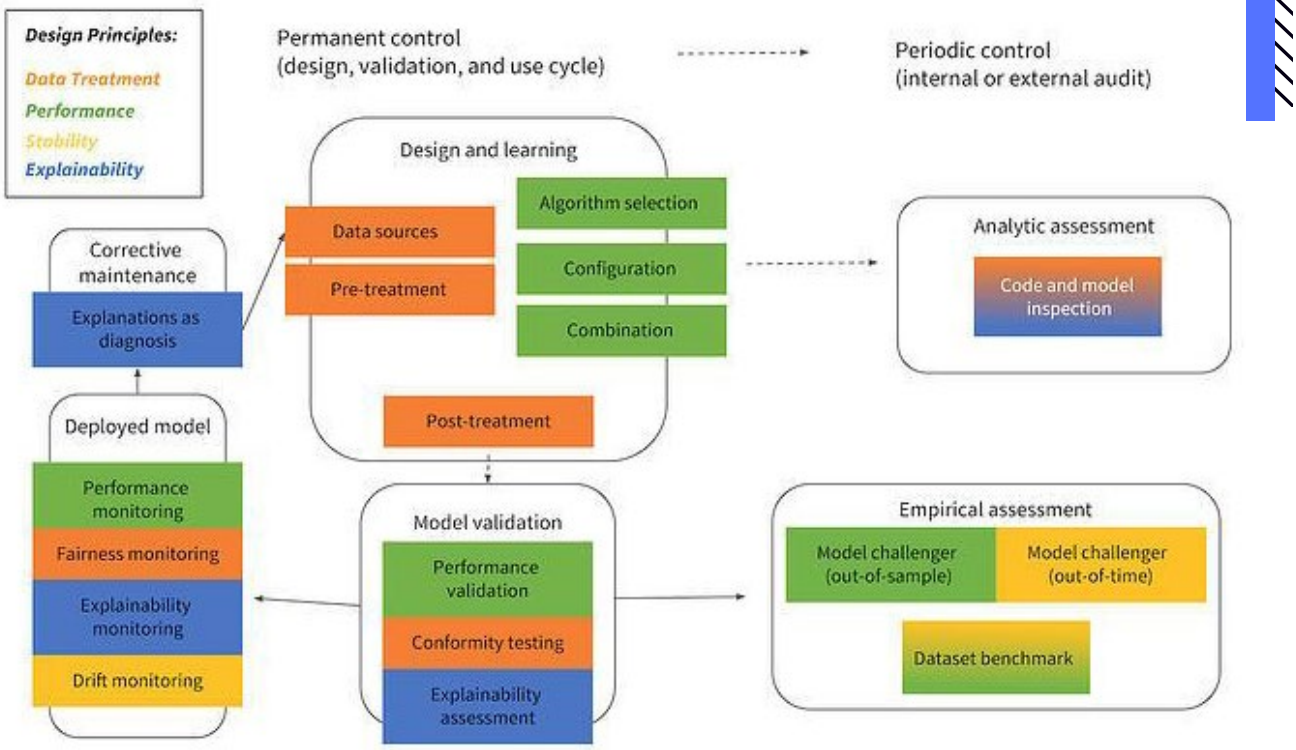


Figure 2. Table from the ACPR paper sketching the cycle of assessment and governance for AI algorithms, with a color code for each main risk criteria. The translation to English was done by Dataiku.

What Does This Mean for Organizations Scaling AI?

The ACPR document nicely fills the applicability gap between regulator debates and organizational reality and provides quick wins for any organizations who wish to accelerate their AI Governance journey. Implementing the ideas outlined above can be time consuming and resource heavy. Building a sense of control over the risks of an increasing number of AI projects can seem like a nearly impossible task. The role of platforms like Dataiku is to make it easier.

In this case, Dataiku does so not only by centralizing data access, modeling techniques, deployment APIs, and collaborative features but also by providing strong oversight over existing AI risks and available controls. Dataiku allows users to view the projects, the models, and the resources that are being used and how. There is model audit documentation to help understand what has been deployed, in addition to full auditability and transferability of everything from access to data to deployment, for each and every project everyone works on.

As a supplier of an AI solution, we leave it to our customers to define and develop their own AI frameworks, but at the same time, we provide the technology and tools to govern AI and comply with upcoming regulation.

Zooming in on Canada

In this section, we are focusing on the recently introduced Bill C-11, also known as the Canadian Federal Data Privacy and AI Regulation bill. Bill C-11 largely reflects the recommendations of the national Data Privacy Regulator (OPC) and sets a precedent in the government's ambition to better manage risks linked to AI. The bill is not law yet, it still needs to proceed through committee review and probably industry consultation throughout the year.

Please note that in this ebook, we will not be covering Quebec's Bill-64[30] which primarily focuses on replicating the already active European Data Privacy regulation (GDPR). For context, the OPC is the Office of the Privacy Commissioner, meaning the administrative authority responsible for overseeing the compliance of the two federal privacy laws. One for the public sector, the Privacy Act, which covers the personal information handling practices of federal government departments and agencies and one for the private sector, the Personal Information Protection and Electronic Documents Act (PIPEDA).[31]

Reforming the Existing Data Privacy Law to Address the Disruptive Nature of AI

The recommendations released[32] by the OPC in November 2020 are the result of a two-year long process driven by the OPC's conviction that, while AI can drive significant benefits, it also presents fundamental challenges to data privacy principles. One of the outcomes is the decision to revisit Canada's main data privacy law, known as PIPEDA (Personal Information Protection and Electronic Documents Act), which defines dos and don'ts on the consensual collection, processing, and analysis of personal information for commercial purposes.

Why?

As part of their work, the OPC identified that the current data privacy regulation does not satisfactorily apply to AI systems in the private sector. Among key concerns is the very nature of AI systems (systems that require large volumes of data to function effectively), which can easily contradict fundamental data principles like minimization (i.e., data collected and processed should not be held or further used).

[30] *http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html*
[31] *https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/*
[32] *https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201112/*

Similarly to other data regulators[33] around the world, the OPC also expresses concerns on the capacity for AI to drive decisions which can deeply affect citizens, raising privacy risks, unlawful bias, and discrimination.

How?

To confirm the initial PIPEDA reform proposals[34], the OPC initiated a public consultation[35] in January 2020 to collect feedback from both field experts and civil society on how to address AI challenges with regulation. After 86 submissions, two in-person consultations, and a policy report[36], the OPC published key recommendations[37] on Nov. 13, 2020 for regulating AI systems (details to follow below).

What is the impact?

The recommendations of the OPC were later used to support the introduction of the Canadian privacy law reform bill in Parliament, also known as the Bill C-11[38]. This upcoming law enacts the OPC recommendation through the Consumer Privacy Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act. They both create new regulatory tools to address compliance, remedies for non-compliance, and a tribunal to address appeals to these remedies. Let's find out what this all means for the usage of AI systems by the private sector in Canada!

How the Bill C-11 Is Expected to Deeply Reshape AI Usage in Canada

The recommendations of the OCP were nearly all included within the Bill C-11 and fall into two categories:

Data Protection

Aligning with existing data protection regulations,[39] the Bill C-11 redefines modalities and exceptions for data collection consent (see a reminder below), sets new data principles (data portability and mobility), and establishes privacy-preserving techniques (de-identification).

[33] *https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/*
[34] *https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/*
[35] *https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200128/*
[36] *https://www.mcgill.ca/channels/channels/news/ignacio-cofone-authors-policy-report-office-privacy-commissioner-canada-326244*
[37] *https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/*
[38] *https://www.ourcommons.ca/DocumentViewer/en/43-2/house/sitting-29/order-notice/page-11*
[39] *https://gdpr-info.eu/*

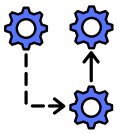
Introducing AI Regulation

The Bill C-11 is the first-of-its-kind in its introduction of regulatory tools for AI, including new rules for automated decision systems as well the regulators' ability to audit organizations and write fines.

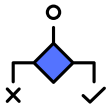
1. Modalities for Collecting, Processing, and Analyzing Personal Information

Here are the modalities for obtaining consent and when consent is not needed:

When to collect consent: Private organizations can collect personal information only with consent before or at the time of collection or before any new use or disclosure of such information.



What information should be shared to obtain consent: Any time consent is collected, the organization must notify individuals in plain language of the type of personal information that the organization collects, uses, and discloses, and of the purposes, manner, and consequences of the collection, use, and disclosure.



What information should be shared to maintain consent validity: Organizations must have (at any time) information, again in plain language, that explains their policies and practices put in place to fulfil their CPPA obligations. Organizations must also identify any third parties to whom personal information will be disclosed.

Exception to consent: Consent doesn't need to be collected either when the personal information is de-identified, when the personal information is transferred to service providers, or when consent is impractical to collect for public interest or legitimate purposes.

2. Rules for AI Design

Conversely to the GDPR, the Bill C-11 establishes a right to explanation both for AI systems that would replace the judgment of a human decision maker but also assists such decisions. The scope of the explanation includes why the decision, recommendation, or prediction was made as well as how the individual personal information was used.

Organizations must also describe in their policies any automated decision system that could have significant impacts on individuals and ensure it is both auditable and offers suitable levels of explainability.

What does it mean for organizations? It widens corporate compliance of AI projects. For example, when the bill C-11 would become law, any recommender system currently leveraged to assist decisions in the financial services, the retail industry or life sciences would require compliance. Besides, organizations need to be able to track and retrieve information easily, especially regarding impact assessments.

3. Potential Fines for Non-Compliance

The Bill C-11 is a page turner for organizations when it comes to its enforcement model. Non-compliance with federal privacy law can ensue a penalty of $10,000,000 and 3% of the organization's annual gross global revenue and up to $25,000,000 and 5% of an organization's annual gross global revenue for more important breaches.

How does it work? The Commissioner has the power to recommend a penalty after an audit and the newly established Personal Information and Data Protection Tribunal imposes the penalty to the organization. The Commissioner can also impose an order in specific cases without the tribunal. These orders can yet be appealed to the tribunal within 30 days.

What are the rights and obligations for organizations that collect and use data? Organizations have a private right of action to premise recourse to the courts in certain circumstances. While the Bill C-11 is not yet law, it gives a solid indication of where Canada is heading and should be a powerful signal to organizations on the need to reinforce their frameworks on AI.

What Does This Mean for Organizations Scaling AI?

It's only the beginning! The Bill C-11 is likely to be modified as it moves forward with the legislative process but binding regulation seems inevitable, especially since there are more OPC recommendations to be implemented, like the right to contest AI decisions and the need to conduct privacy impact assessments.

Although we are only at the beginning of AI regulation compliance, we observe a strong incentive system for organizations to start thinking through AI Governance. What does it mean for my organization? What kind of resources do I need? More people, more processes, more technology? All three?

If we take Bill C-11's right to explanation as a compliance example, it can be challenging for organizations to deliver AI explanations and data reporting without the right processes or the right people to design them. If we also think that there is more than one AI system in need of compliance, manual processes might be not enough. The role of platforms like Dataiku is to help organizations understand how they work with data and build AI systems to later provide best-in-class explanation and data reporting.

Zooming in on Singapore

In this section, we're focusing on the operational guidelines spearheaded by Singapore's Personal Data Protection Commission (PDPC), which is Singapore's main authority body for administering the Personal Data Protection Act (PDPA), 2012. Starting in 2019, the regulator's approach to AI Governance has been incredibly forward thinking: they have fostered guideline adoption for 200+ organizations by delivering actionable governance best practices and real-life implementation examples.

The Singaporean frameworks outline fundamental principles and detailed guidelines to support any organization in getting up to speed with AI Governance. Governing AI will soon become a must-do under the push of AI-specific regulations, such as the Draft Artificial Intelligence Act set by the European Commission. The "why" of AI Governance is now evolving to a "how," and the framework created by Singapore provides you with a powerful baseline from which to build.

Step 1: A Universal AI Governance Framework Already Adopted by 200 Organizations

Remember the self-regulatory stance of the U.S.? The Singaporean government holds similar beliefs. Yet, their self-regulatory stance is not leading to the Wild West of AI.

What? How is this possible? The PDPC outlined detailed guidance that is readily implementable for the private sector. In other words, a step-by-step guide for AI Governance and compliance. Such a framework stands the test of time, as it has been updated through public and industry consultations and completed with further guidance and references to ease adoption.

Singapore's AI Governance Framework

In 2019, the PDPC released[40] the first edition of the Model AI Governance Framework (MAIGF) at the World Economic Forum (WEF) in Davos, Switzerland. It was already positioned as a "living document" open to industry and institutional feedback to be reviewed in a couple of years.

It's the first piece of guidance on AI Governance in Asia and aims to be:

- Algorithm agnostic: It caters both to AI or data analytics methods.
- Technology agnostic: It applies regardless of the development language and data storage method.
- Sector agnostic: It serves as a baseline set for organizations that encourages sector-specific considerations and measures.
- Scale and business model agnostic: It does not focus on scale or size.

The framework is centered around two guiding principles, four areas of guidance, and real-life examples, all of which are outlined below:

1. AI systems should be human-centric (i.e., ensure humans can easily interact with the system) and their decisions should be explainable, transparent, and fair.
2. These principles should be translated into (a) internal governance structures and measures, (b) processes gauging human involvement in AI-augmented decision making, (c) operations management, and (d) stakeholder interaction and communication.

[40] *https://www.straitstimes.com/singapore/singapore-releases-model-governance-framework-for-ai*

MAIGF's four areas of guidance [41]

3. Real-life examples from world-renowned organizations (i.e., Mastercard, Facebook, Merck Sharp & Dohme, etc.) on how to best implement the guidance. For example, how a probability versus severity of harm matrix was used to assess harm and the appropriate degree of human intervention.

[41] *https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework*

GRAB:

ILLUSTRATION ON DETERMINING THE LEVEL OF HUMAN INVOLVEMENT IN AI-AUGMENTED DECISION-MAKING

Grab is a Singapore-based company that offers ride-hailing transport services, food delivery and e-payment solutions. It uses AI across its platform, from ride allocation, detecting safety incidents, to identifying fraudulent transactions. In particular, Grab uses AI to improve the overall quality of trip allocations and minimise trip cancellations.

To allocate trips successfully, Grab's AI model considers drivers' preferences based on the following key factors:

a. Driver's preferences for certain trip types;

b. Preferred locations where a driver start and end their day; and

c. Other selective driving behaviours.

In determining the level of human involvement in its AI's decision-making for trip allocation, Grab considered the following key factors:

a. The scale of real-time decision-making required. As Grab has to make over 5,000 trip allocations every minute, this would mean an impact to customers in terms of efficiency and cost if a human had to review each trip allocation; and

b. The severity and probability to users should the AI model work in a sub-optimal manner.

Among other factors, Grab considered that: (1) it is not technically feasible for a human to make such high volume of trip allocations in a short amount of time; and (2) there is often little or no harm to life should there be less than optimal trip allocations. Hence, Grab decided to adopt a human-out-of-the-loop approach for its AI model deployed for trip allocation, while continuously reviewing the AI model to ensure optimal performance.

MAIGF's real-life example on determining the level of human involvement in AI-augmented decision making [42]

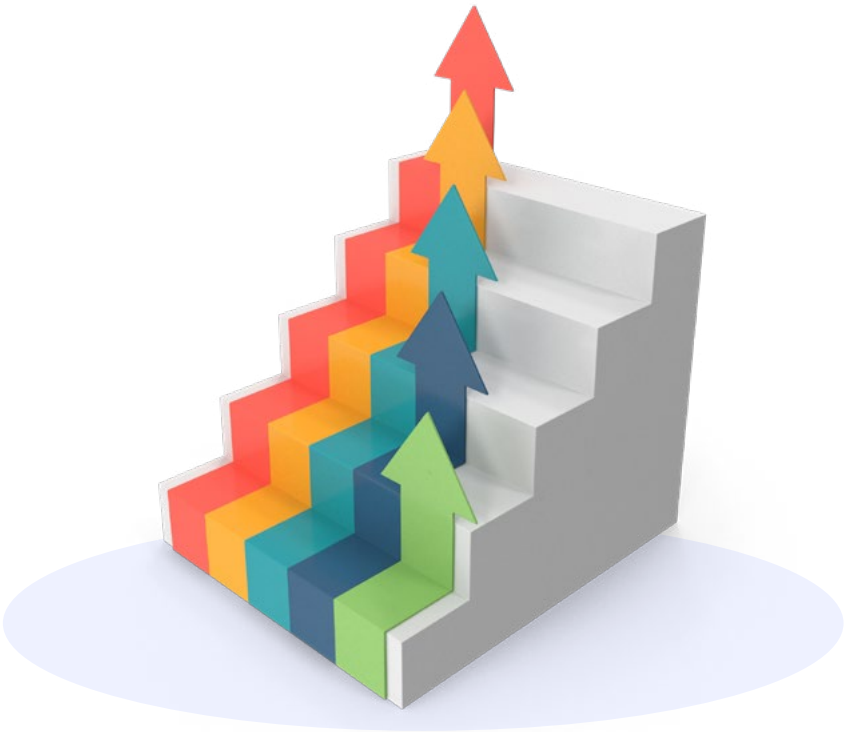
[42] *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf*

Following the first release in 2019, PDPC released a second version of MAIGF[43] in 2020 with more industry examples and conceptual clarifications (the primer is also accessible here[44]). The second release also included:

- A guide to implement MAIGF[45] in collaboration with WEF's Center for the Fourth Industrial Revolution and a contribution of 60 organizations.

- Two volumes of use cases (here and here) to demonstrate how local and internal organizations across different sectors and sizes implemented or aligned their AI Governance practices with all sections of MAIGF.

It's a lot of content, and one might feel overwhelmed at first glance, yet PDPC has supported nearly 200 accounts on how this governance model can be implemented and how it brings value to private organizations. Whether as a reflection piece or a fully integrated framework, the MAIGF helps democratize AI Governance practices and creates a culture for efficient and responsible innovation. But wait, there's more!



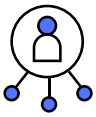
[43] *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf*
[44] *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Primer-for-2nd-edition-of-AI-Gov-Framework.pdf?la=en*
[45] *http://go.gov.sg/isago*

Step 2: AI Governance for Financial Services

In 2018, the Monetary Authority of Singapore (MAS) developed its own AI Governance guidelines. They are naturally more extended and precise than PDPC's as they are targeted at the financial actors of Singapore. They provide a very good example for how the MAIGF could be completed in or adapted to a specific sector.

First, MAS released the *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector*[46]. The document lists 14 principles specific to financial products and services around four main concepts (FEAT):

Fairness:
AI systems' use should be justified and reviewed.



Ethics:
AI-driven decisions should be held to human-driven decisions standards.

Accountability:
AI systems should be accountable internally and externally.

Transparency:
AI systems and how they are built should be explained to increase public confidence.

These principles have paved the way for a dedicated framework, Veritas, to promote the responsible adoption of AI and data analytics in financial services[47].

This framework is particularly relevant because it addresses the implementation challenges for the FEAT principles.

[47] *https://www.mas.gov.sg/news/media-releases/2020/fairness-metrics-to-aid-responsible-ai-adoption-in-financial-services*

The first phase of the project aims at addressing the Fairness principles:

- The first edition focuses on the development of fairness metrics for popular use cases with a high propensity for bias, like credit risk scoring and customer marketing. Again, this framework is developed with the help of a consortium that gathers key actors like HSBC or United Overseas Bank (UOB).
- The second edition[48] focuses on building similar metrics for two insurance use cases: predictive underwriting and fraud detection.

The white papers and the open source code for the first edition are available for viewing and phase two of the Veritas cycle on tackling FEAT's ethics principles is already planned.

Although MAS work delivery is less extensive than PDPC, it is still very impressive. Looking back on the section on France earlier in this ebook, we can observe a trend emerging across national financial services actors anticipating upcoming regulation by adopting an operational approach to AI Governance and compliance.

[48] *https://www.mas.gov.sg/news/media-releases/2021/veritas-initiative-addresses-implementation-challenges#1*

Step 3: Reflecting on How These Frameworks Fit Within the Larger Galaxy

The Singaporean frameworks are one of many. If you haven't found what you were looking for, there are more frameworks to start building AI principles and implement them successfully (as evidenced by this ebook).

If there is one thing to learn from this section it's that this framework is another move toward updating the governance framework and structure of AI. Simply put, it's another market signal that AI Governance is transitioning from a research trend to a corporate standard. All initiatives are different but ultimately, they all have the same demand from private players when it comes to AI: establish a structure to identify core principles and enforce them in your AI project lifecycle.

There is a second thing to learn here. You might be wondering why I am spending so much time delving into AI regulation around the world in the name of Dataiku. The answer is pretty straightforward — without AI principles and their initial implementation within a governance framework, it's difficult to leverage any governance platform capabilities. If you don't know what risks you are looking at, it's difficult to address them with the appropriate tooling.

Then comes the tooling question. Dataiku's role is to help companies build and deploy AI at scale. Initially, it leverages the platform logic to centralize data efforts across teams to empower them to deliver more projects.

Such logic is also applicable to governance as it helps addressing fundamental stakes regarding AI:

- Where are my models?
- How are my models performing?
- Are my models aligned with my business objectives and principles?
- Do the models carry any risks for my organization?

Governance is the next logical step to build resilience in AI and address the new set of guidelines and regulations. Dataiku has key capabilities to operationalize existing AI Governance guidelines and navigate the upcoming regulatory environment.

Conclusion

Phew! We know that was a lot but, as you can see from the chart below, it only scratches the surface of AI regulation (and therefore AI Governance) around the world.

AI Regulation Around the World

Global Perspective

G : Guidelines
C : Consultation
D : Direction
R : Regulation

data iku

Countries/ Organisations	Stage	Focus	Coming Next
Europe	G C D R	• **European Commission** creates a values-based framework with **wide-ranging AI definition, bans for specific applications, obligations for high-risk AI developers/users, recommendations** for remaining use cases **with up to 30MnE fines** • **European Parliament** will play a critical role in amending the AI Act and provides policy views on existing law (GDPR) and AI. • **Council of Europe** extends beyond EU and is developing a **legal framework to regulate AI**, though operationalization is unclear.	**EC** Proposal **being discussed** for a 2022 implementation **CoE** negotiating content and mechanism.
Canada	G C D R	• **Binding private sector privacy framework** including AI explainability • **Regulator can require demonstration of compliance** and issue **fines** • Largely inspired by EU regulation and discussions	**Bill C-11 in revue**
UK	G C D R	• UK AI Council AI Roadmap **released in Jan 2021.** Appeal for increased investments and governance. • Longstanding position that AI regulation should prioritize verticals or sectors, avoiding 'blanket' or a European approach. • Regulators working to fit existing law and regulation to AI, thematic consultations conducted and more expected. • New and impending guidance for AI to conform to existing law and regulations, e.g. ICO & Data Protection Act 2018.	New proposals from Office for AI and regulators likely. More guidance on regulation and AI expected.
United States	G C D R	• **Federal guidelines** issued to prepare ground for industry-specific guidelines or regulation • Focus on public trust and fairness. No broader ethics considerations. • Numerous and diverse state-level efforts to regulate AI, demonstrating federalisation of issue and perceived relevance of bias, discrimination, and transparency.	FTC plans to go after companies using and selling biased algorithms
Australia	G C D R	• **Detailed guidelines issued,** integrating ethical and a strong focus on end-customer protection	Further guidance
Singapore	G C G	• **Positive, non-sanction-based** approach focusing on practical steps and best practices to implementing AI governance at an organization level. • Any B2C Model should be explainable, transparent and fair	
UNESCO	G C G	• **Global recommendations** for member states to build common standards on AI Regulation • Focus on human rights and SDGs achievements • Non-binding but will likely inform how governments think about governing AI domestically.	**Member state** adoption planned for November Conference
OECD	G	• 42 signatories • 5 principles for responsible stewardship of trustworthy AI: inclusive growth; human-centred and fairness; transparency and explainability; robustness; accountability. • Recommendations for national policies	

As your organization begins thinking about (and then implementing) an AI Governance strategy, it is our hope that you utilize these best practices — hand-in-hand with MLOps and Responsible AI — as a baseline to sustain the growth of your AI projects. Addressing these issues too late in the game can not only lead to AI Governance debt and productivity lost, but more grave implications such as operational risks and legal compliance concerns.

About the Author

Paul-Marie Carfantan

Paul-Marie Carfantan is a manager for AI Governance solutions at Dataiku. He's responsible for the regulatory watch as well as the design and implementation of methods and solutions to govern AI at scale. Besides co-developing Dataiku's offering for robust and efficient AI Governance, he acts as the go-to-person on AI Governance-related topics. Paul-Marie builds on years of experience researching, contributing to think tanks, and consulting in the field, notably at Deloitte France and the London School of Economics.

Contributors

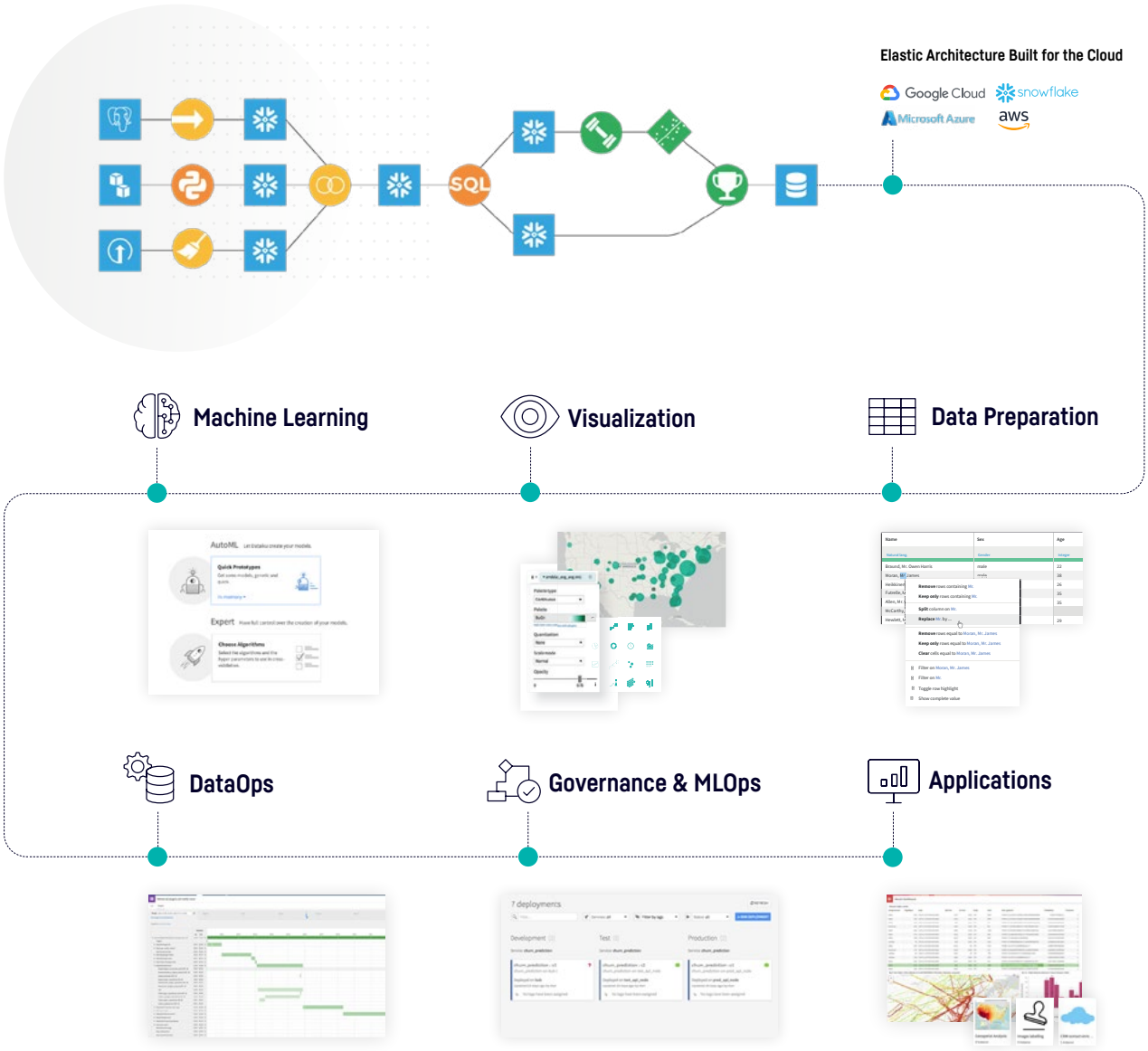
Sophie Dionnet

Sophie is the General Manager, Business Solutions at Dataiku where she drives the development of industry-specific solutions and AI governance offers to support robust and efficient AI scaling. She has 14 years of experience in the asset management industry and notably acted as COO for a multi-asset portfolio management division, conducting large scale IT, regulatory, and transformation projects, including active development of responsible investment.

Jacob Beswick

Jacob Beswick is Dataiku's Senior AI Governance Solutions Manager. Prior to joining Dataiku, Jacob worked in the U.K. Government's Office for Artificial Intelligence where he led portfolios on AI adoption, AI regulation, and governance. With this background, Jacob brings insights on external requirements that AI developers and users will face going forward and best practices for operationalizing AI ethically and responsibly.

Everyday AI, Extraordinary People



450+
CUSTOMERS

45,000+
ACTIVE USERS

Dataiku is the world's leading platform for Everyday AI, systemizing the use of data for exceptional business results. Organizations that use Dataiku elevate their people (whether technical and working in code or on the business side and low- or no-code) to extraordinary, arming them with the ability to make better day-to-day decisions with data.

EBOOK

www.dataiku.com