securiti

Building a Framework for AI Governance

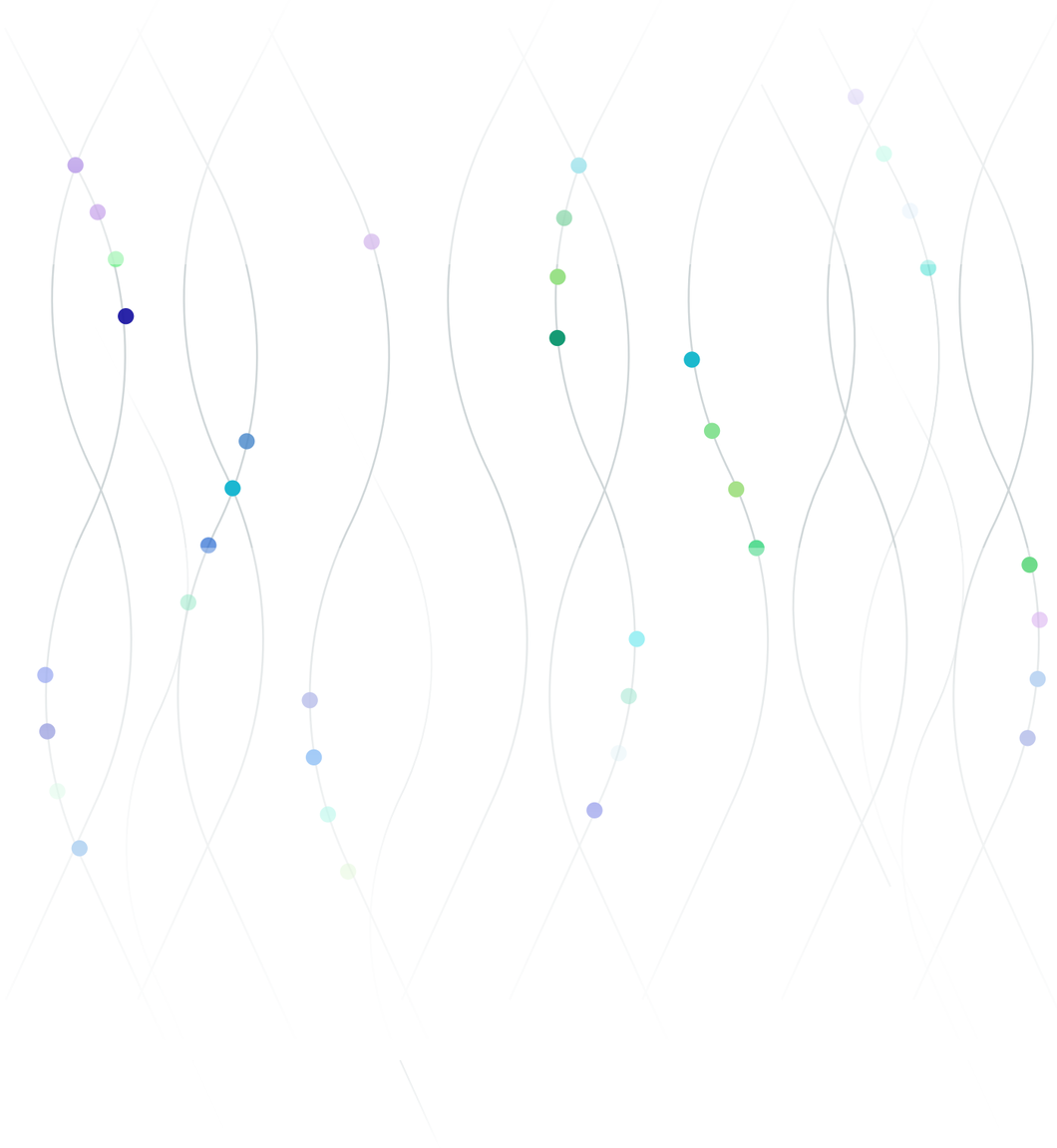
Content

The value of Artificial Intelligence

The unparalleled opportunities offered by the rapid development of artificial intelligence (AI) systems and models in the last year, after the launch of ChatGPT in November 2022, has electrified the business world in a way that has never been seen before.

From automating routine tasks to increase productivity and efficiency, to uncovering deep insights hidden within vast datasets, to providing creative output and inspiration from the most vague of briefs, to generating quality content at astronomical scales at bewildering pace, to providing reasoned, rational and auditable autonomous decision-making, to piloting drones and cars: the promise offered by AI to the business world is unrivaled in its scope and scale and it offers a paradigm shift in how the business world will operate.

It is estimated by Mckinsey that just Generative AI (a subset of artificial intelligence models - i.e applications such as ChatGPT, GitHub Copilot, Stable Diffusion, and others) could add the equivalent of $2.6 trillion to $4.4 trillion annually to business revenues with more than 75% of value arising from the embedding of Generative AI for the purposes of Customer operations, marketing and sales, software engineering, and R&D.



The risks posed by Artificial Intelligence

As the immense and unprecedented value offered by the development of AI systems and models is being realized by the business world, the immediate dangers and risks posed by the unregulated development of this technology are also becoming increasingly the topic of conversation in the global milieu.

The very characteristics which make AI systems and models such as LLM models attractive technological innovations also make them potentially the riskiest technology if not developed and implemented cautiously.

Specifically focusing on current AI systems and models ability to discern patterns, predict behaviors, and draw insights from vast troves of information exposes vulnerabilities that, if exploited, can lead to:

Unauthorized surveillance of persons and human societies on a massive scale,

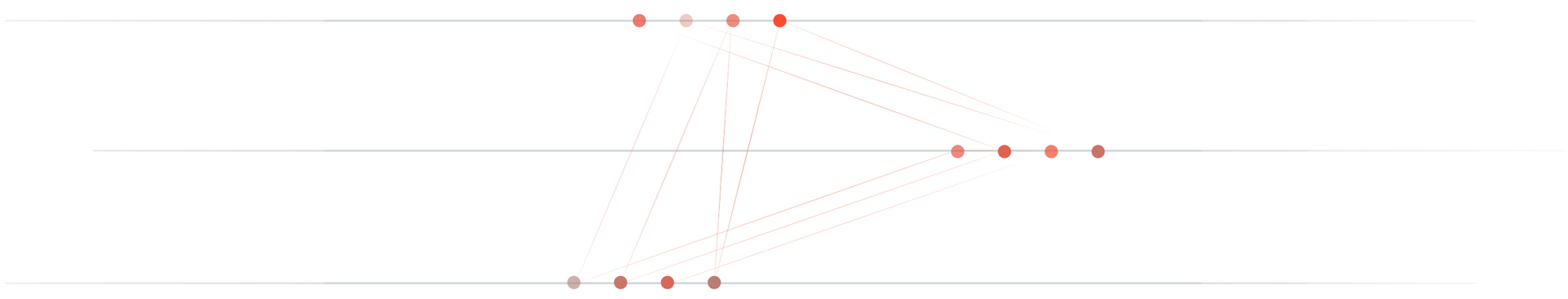
Unexpected and inadvertent breaches of personal information of individuals,

Manipulation of personal information of massive populations for an uncountable number of processes,

Inherent bias, racism and prejudice for legal and socially significant outputs,

Deeply invasive and accurate psychological and behavioral profiling of individuals.

The risks posed by the rapid development of AI systems and models are considered so acute that In March 2023, in an unprecedented development, 30,000 people, including some of the top technologists and technology business leaders in the world signed a letter asking for global governments and regulators to intervene unless AI developers agreed to a voluntary 6 month halt or slow down in the development of AI technology.



Why understanding AI Regulation is important

With the proliferation of AI models and systems in the business and commercial world and rapid development and innovation in their capabilities and use cases, governments and legislators are moving fast to develop regulatory controls to ensure privacy and other related risks posed by these AI models and systems are identified, mitigated and regulated before any significant type of harm is causes. This proactive global response to AI systems and models is marked by a concerted effort to strike a balance between technological innovation, business potential, individual rights and overall societal good.

Governments and regulators are also not shy to spring into action if any AI system or model enters into controversy:

Clearview AI

Clearview AI, a US company which developed an AI facial recognition algorithm based on photos scrapped from social media websites, was recently fined almost $8 million by the UK's Information Commissioner's Office for collecting personal data from the internet without obtaining consent of the data subjects. Similarly, the Italian data protection authority fined the company $21 million for committing breach of data protection rules. The authorities in Australia, Canada, France, and Germany have also taken similar enforcement actions against the company. In the United States, through a lawsuit brought by the American Civil Liberties Union (ACLU) under the Illinois's Biometric Information Privacy Act (BIPA), Clearview AI consented to stop selling its AI facial recognition algorithm system in the United States to most businesses and private firms across the U.S. The company also agreed to stop offering free trial accounts to individual police officers, which had allowed them to run searches outside of police departments' purview.

Replika AI

The Italian data protection authority banned the Replika app, an AI chatbot developed by Luka Inc., from processing personal data of the Italian users. The company was also issued a warning to face a fine of up to 20 million euros or 4% of the annual gross revenue in case of non-compliance with the ban. The reasons for the ban cited by the regulatory authority included concrete risks for minors, lack of transparency, and unlawful processing of personal data.

ChatGPT

ChatGPT, a large language model-based chatbot developed by OpenAI, was banned by the Italian data protection authority and was only allowed to resume its operation once it established controls to comply with the GDPR provisions related to privacy notice, legal bases for data collection, and the data subject rights. Further, data protection authorities in Canada, Spain, Germany, and Netherlands have also initiated or have shown intention to initiate investigation proceedings to check the chatbot's compatibility with data protection laws.

Thus, while the potential profitability of developing, using and deploying AI solutions is undeniable for global businesses due to the promised enhanced efficiency, unprecedented insights, and transformative growth offered by the technology, however, the regulatory landscape surrounding AI remains a tumultuous frontier, where vague legal frameworks and evolving global standards developing in real time create a unique compliance challenge and a risky business environment filled with potential liabilities. Thus, in this unmapped and uncharted landscape, businesses are confronted by the imperative to work hard to be the first to develop and deploy this game changing technology while navigating the regulatory maze carefully so as not to risk massive liabilities. Therefore, in such a pivotal juncture, the value of gaining insights into the regulatory obligations envisioned by global regulators cannot be overstated.

Mapping AI Regulatory Compliance Obligations

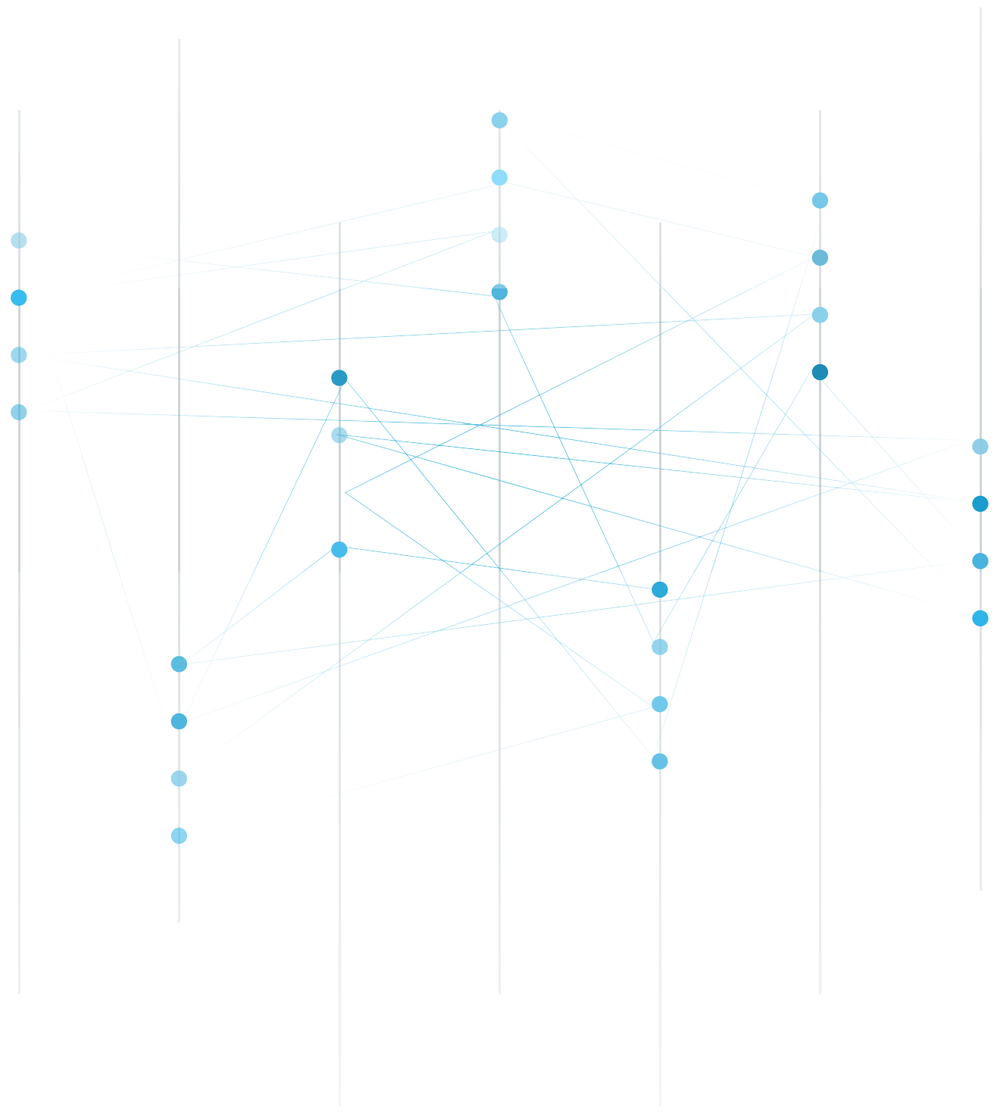
Securiti has taken the lead in mapping the obligations which will be placed on AI systems and models and boiling them down into 25 operational requirements divided into 6 operational categories which will be required to be implemented by global businesses looking to develop, use or deploy AI systems and models.

Our team of privacy researchers have synthesized these obligations by studying and analyzing existing and well known privacy legal frameworks, working papers and guidances and major legislative/regulatory efforts which are nearing finalization by some of the most influential global regulators in three of the biggest markets in the world, all of which will see massive adoption of AI technologies:

The European Union's General Data Protection Regulation (GDPR) and draft Artificial Intelligence Act (AI Act)

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and draft Artificial Intelligence and Data Act (AIDA)

The United State of America's Federal Trade Commission's guidances on AI and the US White House's Blueprint for an AI Bill of Rights (AI Bill of Rights)



While the European Union's GDPR and Canada's PIPEDA are currently in effect, the AI Act is expected to come into force by the end of 2023. The majority of the provisions of the AI Act will apply 24 months after its passage by the European Parliament, during which time companies and organizations will have to ensure that their AI systems comply with the requirements and obligations set out in the regulation. On the other hand, Canada's AIDA passed its second reading at the House of Commons on 27 April 2023 and is still under consideration with the Standing Committee on Industry and Technology.

The United States Federal Trade Commission is the forefront agency tackling AI development regulation and has taken major regulatory actions against AI developers in the United States and has released a treasure trove of guidance for the safe and ethical development and use of AI systems and technology - these guidelines are further backed by the White House Blueprint of an AI Bill of Rights, a guidance document to help guide the design, use, and deployment of automated systems to protect the American Public. The principles are non-regulatory and non-binding but will be influential in any future AI regulatory efforts within the US.

It is important to note that majority of laws researched by us are taking aim at two major types of AI systems being developed and launched across the world for a variety of commercial and other applications: Generative AI Models (LLMs) and Automated Decision Making (ADM) AI Models - both types of AI systems process 'personal data' of individuals to function and thus are considered to pose privacy risk for data subjects and other risks for society at large, however, other AI models can also fall within the purview of these legislations. We have also focused on charting out the regulatory requirements which will be imposed on both AI developers and users.

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights

1 GOVERNANCE

	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
1.1	**AI System Classification** You are required to classify your AI system and document the reasons for such classification.	**AI Act** Articles 6	**AIDA** Section 7 Section 10(1)(b)	
1.2	**AI Logic Audit** You are required to document and monitor your AI system's logic and factors that it uses to achieve end results.	**GDPR** Article 13.2(f) Article 14.2(g) Article 15.1(h		
1.3	**AI System Data Mapping** You should be able to map the data assets, processes, vendors and third parties involved with the AI Data System.	**AI Act** Articles 10		
1.4	**Training Data Classification** You need to know, classify and document and monitor what data is being processed by the AI system (classify the data. record its source etc.)	**AI Act** Articles 6		
1.5	**Data Governance Controls** You must ensure that data/ personal data being used in AI system adheres to principles of data minimization, purpose specification, data retention	**GDPR** Articles 5 **AI Act** Articles 10	**PIPEDA** Schedule I, Sections 4.2, 4.4, 4.5	**AI Bill of Rights**

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
1.6	**Training Data Controls** You need to be able perform certain operations on the data/personal data being used to train the AI System (bias removal, anonymization).	**AI Act** Articles 10	**AIDA** Section 6	**AI Bill of Rights** FTC: Aiming for truth, fairness, and equity in your company's use of AI FTC: Using Artificial Intelligence and Algorithms
1.7	**AI Output Filters** You need to be able to monitor output results in real-time to detect any release of personal data in the output results.	**GDPR** Article 4(12) Article 33 & 34	**PIPEDA** Section 2(1) Section 10.1-10.3	**GDPR** GDPR Articles 5 AI Act Articles 10
1.8	**ROPA Reports** Regulators can audit the use of data/personal data used in AI systems (An AI ROPA report).	**GDPR** Articles 30	**AIDA** Section 13	
1.9	**Algorithm Deprecation/ Disgorgement** You must be able to retain versions of the AI system to be able to deprecate/claw back/disgorge the AI algorithm by removing illegal data and the learning obtained from it.	**AI Act** Articles 10	**AIDA** Section 6	**AI Bill of Rights** FTC: California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App FTC: FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
1.10	**AI Event Logs** You must keep the logs (automatic recording of events) for an appropriate period of time based on the intended purpose of the AI system and must be able to provide access to the regulatory authority to these logs upon request	**AI Act** Article 12 Article 16 Article 20 Article 23 Article 25 Article 26 Article 29		
2	**DISCLOSURE REQUIREMENTS**			
2.1	**Disclose use of data for AI in Privacy Notice** You must explain the logic of the AI system, the factors relied on the AI system in making the decision.	**GDPR** Article 13.2(f)	**PIPEDA** Schedule I, Section 4.8 **AIDA** Section 11	**AI Bill of Rights** FTC: Aiming for truth, fairness, and equity in your company's use of AI FTC: Using Artificial Intelligence and Algorithms
2.2	**Disclose logic of AI system in Privacy Notice** You need to be able to monitor output results in real-time to detect any release of personal data in the output results.	**GDPR** Article 13.2(f) Article 14.2(g)	**AIDA** Section 11	**AI Bill of Rights** FTC: Using Artificial Intelligence and Algorithms
2.3	**Disclose rights of data subject in reference to AI in privacy notice** You must also inform the data subject about their right to an human review appeal/opt-out and right to delete data from the AI system (as a best practice requirement).	**GDPR** Articles 13.2(b)		

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
3	**DSR REQUIREMENTS**			
3.1	**Right to opt-out of Automated decision making/profiling** Data subjects need to be provided an opportunity to opt-out of automated decision making.	**GDPR** Article 21 Article 22		**AI Bill of Rights**
3.2	**Right to appeal automated decision** Data subjects need to be provided an opportunity to appeal any automated decision making and ask for a human review.	**GDPR** Article 22		
3.3	**Right to access in context of AI systems** As a best practice, data subjects must be provided an opportunity to access their personal data being used or has been used by AI systems.	**GDPR** Articles 15(h)	**PIPEDA** Schedule I, Section 4.9	**AI Bill of Rights** FTC: Using Artificial Intelligence and Algorithms
3.4	**Right to delete in context of AI systems** As a best practice, data subjects must be provided an opportunity to have their personal data deleted from AI systems and any other database which will be used by an AI system.	**GDPR** Article 17		**AI Bill of Rights**

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
4	**CONSENT REQUIREMENTS**			
4.1	**Informed Consent** If you are relying on consent as a legal basis to use personal data of data subjects in an AI system, you must obtain informed consent (see disclosure requirements).	**GDPR** Articles 6 & 7	**PIPEDA** Schedule I, Section 4.3	**AI Bill of Rights**
4.2	**Right to opt-out of Automated decision making/profiling** Data subjects must have the right to opt-out of automated decision making (see DSR requirements)	**GDPR** Article 21 Article 22		**AI Bill of Rights**
5	**ASSESSMENTS**			
5.1	**AI Classification Assessments** Obligations related to AI Systems may differ depending upon its classification, thus you might me required to assess what category it falls under	**AI Act** Articles 6	**AIDA** Section 7 Section 10(1)(b)	

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
5.2	**AI related DPIAs** You must assess and identify the privacy risks posed by AI systems to data subjects and society and document and apply mitigation measures to reduce the identified risks.	**GDPR** Articles 35	**AIDA** Section 8	**AI Bill of Rights** FTC: The Luring Test: AI and the engineering of consumer trust FTC: Chatbots, deep fakes, and voice clones: AI deception for sale FTC: Keep your AI claims in check FTC: Aiming for truth, fairness, and equity in your company's use of AI
5.3	**Algorithmic Impact Assessments** You must assess and identify the risks (other than privacy) posed by AI systems to data subjects and society and document and apply mitigation measures to reduce the identified risks.	**GDPR** Articles 35 **AI Act** Articles 9	**AIDA** Section 8 Section 9	**AI Bill of Rights** FTC: The Luring Test: AI and the engineering of consumer trust FTC: Chatbots, deep fakes, and voice clones: AI deception for sale FTC: Keep your AI claims in check FTC: Aiming for truth, fairness, and equity in your company's use of AI
5.4	**AI Bias Assessments** You must be able to assess AI systems for any inherent bias in their decisions/outputs by conducting equity assessments	**AI Act** Articles 10	**AIDA** Section 8	**AI Bill of Rights**

Req.	Obligations	GDPR and AI Act	PIPEDA and AIDA	US FTC AI Guidance and AI Bill of Rights
6	**SECURITY SAFEGUARDS**			
6.1	**Protect the data** You must protect personal data being used by the AI system through technical measures.	**GDPR** Articles 32 **AI Act** Articles 15	**PIPEDA** Schedule I, Section 4.7	**AI Bill of Rights**
6.2	**Protect the system** You must protect the AI system from unauthorized access, manipulation by bad actors through technical measures.	**GDPR** Articles 32 **AI Act** Articles 15	**PIPEDA** Schedule I, Section 4.7	**AI Bill of Rights**

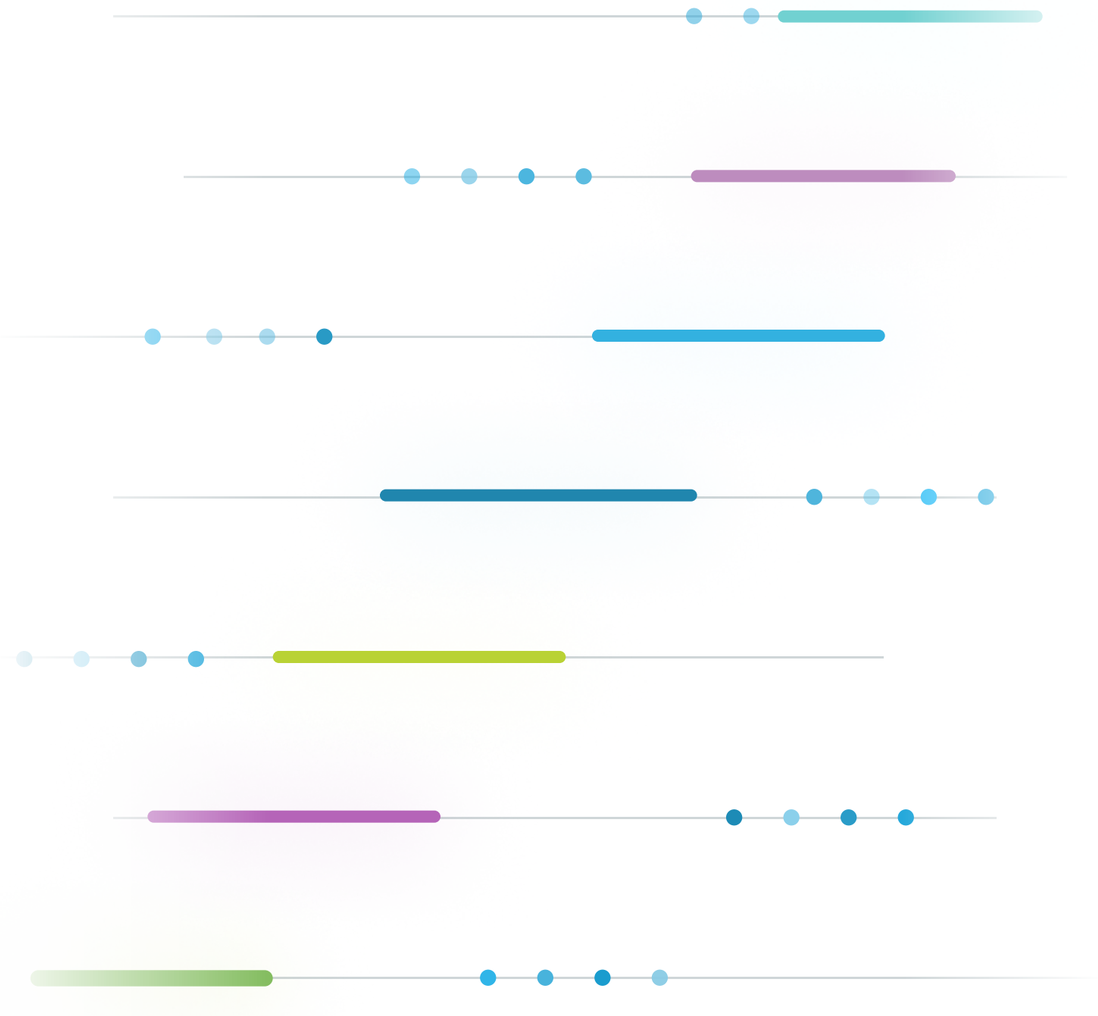
7 Steps AI compliance program

Based on the massive business opportunities coupled with the regulatory risks posed by the development and deployment of AI systems and models, the immediate need for global businesses to establish a robust AI compliance program cannot be overstated.

But where do businesses begin? To ensure consistency, comprehensiveness and accountability, businesses must ensure that AI compliance efforts must be taken in a systematic and structured manner similar to how they employ a privacy program.

By crafting a structured mechanism to navigate this intricate and evolving compliance terrain will not only mitigate risks but also cultivate a competitive advantage by rooting your AI solutions in demonstrable trust, ethics and accountability. By following this step-by-step mechanism and leveraging cutting-edge privacy management software, businesses can confidently navigate the AI regulatory landscape, ensuring adherence to obligations and solidifying their position as pioneers in responsible and sustainable AI innovation.

Our privacy research team, having studied the compliance obligations on AI systems and models by global regulators and synthesizing 25 operational requirements, leveraged our deep institutional knowledge in the privacy management field to develop a 7 step compliance program for AI developers and users looking for actionable insights that can be readily translated into effective strategies to control the regulatory risks these new technologies impose.



STEP	RELEVANT REGULATORY REQUIREMENTS	HOW SECURITI CAN HELP?
STEP 1 **Classify AI systems and Assess risks** Assess the risks of your AI system at pre-development, development and post-development phase and document mitigations to the risks. You must also classify your AI system, do bias analysis etc.	5.1 - AI Classification Assessments 5.2 - AI related DPIA 5.3 - Algorithmic Impact Assessment 5.4 - AI Bias Assessment	Automated Assessments
STEP 2 **Secure AI systems** Ensure there are proper safeguards to protect AI systems and the data involved from security threats, unauthorized access etc.	6.1 - Protect the data 6.2 - Protect the system	Data Security Posture Management Data Access Governance
STEP 3 **Monitor and clean input data** Catalog your training data to ensure bias removal, anonymization, removal of sensitive personal data, remove obsolete data, ensure the data is accurate, ensure data is minimized etc.	1.4 - Training Data Classification 1.5 - Data Governance Controls 1.6 - Training Data Controls	Data Mapping Sensitive Data Intelligence
STEP 4 **Disclose AI system related details to Data Subjects** Publish and AI systems related disclosures to data subjects in your privacy policy with explanations of what factors will be used in automated decision making, the logic involved and the rights available to data subjects.	2.1 - Disclose use of data for AI in privacy notice 2.2 - Disclose logic of AI in privacy notice 2.3 - Disclose rights of data subjects in reference to AI in privacy notice	Privacy Notice Creation & Management

STEP	RELEVANT REGULATORY REQUIREMENTS	HOW SECURITI CAN HELP?
STEP 5 **Take Consent and Honor Opt-outs from Data Subjects** Provide Data Subjects the right to opt-out of their personal data being used by AI systems (or to opt-in or withdraw consent) at time of collection of their personal data.	4.1 - Informed consent 4.2 - Right to opt-out of automated decision-making/profiling	Consent Management
STEP 6 **Fulfill DSRs (Access, Deletion, Appeal/Human Review)** Provide data subjects the right to: *Access their personal data which has been processed by the AI data system, the logic involved and the outputs it created based on the process.* *Delete their personal data from AI data systems and possibly remove an 'learning' from that data from the algorithmic model.* *Opt-out their personal data from an AI system and possibly remove an 'learning' from that data from the algorithmic model.* *Provide the data subject a right to appeal any decision made by an AI system or obtain human intervention.*	3.1 - Right to opt-out of automated decision-making/profiling 3.2 - Right to appeal automated decision 3.3 - Right to access in context of AI systems 3.4 - Right to delete in context of AI systems	Data Subjects Rights Data Mapping

STEP	RELEVANT REGULATORY REQUIREMENTS	HOW SECURITI CAN HELP?
STEP 7 **Demonstrate Compliance and Audit** Monitor the AI system: *Know what personal data / sensitive personal data is fed into it,* *Show that it is complying with its intended logical parameters, bias removal mechanisms etc.* *Demonstrate compliance to regulators.* *Produce ROPA Reports and maintain event logs.*	1.1 - AI System Classification 1.2 - AI Logic Audit 1.3 - AI System Data Mapping 1.7 - AI Output Filters 1.8 - ROPA Reports 1.9 - Algorithmic Deprecation/Disgorgement 1.10 - AI Event Logs	**Data Mapping** **Sensitive Data Intelligence**

Conclusion

The future of the business world in the face of the exponential development and growth of AI systems and models and their capabilities is both promising and perilous, presenting businesses with an unparalleled opportunity for growth, innovation, and enhanced efficiency, alongside a complex web of potential risks and regulatory obligations.

However, the convergence of innovation and responsibility is not just a conceptual ideal but a tangible and practical path forward: by blending the visionary potential of AI with the practical realities of regulatory adherence, businesses can create a symbiotic relationship that fortifies their growth in the upcoming AI race while also upholding their ethical standards and reputations and contributing to a safer and better world. This is where Securiti can help.

Through this report, we have illuminated the multifaceted risks associated with AI, ranging from privacy concerns to ethical considerations, underlining the importance of a proactive approach to compliance. The mapping of upcoming regulatory obligations provides a roadmap for businesses to understand the compliance expectations of major global regulators from AI developers and users. Businesses must begin to develop technical capabilities, policies and procedures to ensure they can continue to develop and use AI systems and models while avoiding potential legal pitfalls which may arise in the future.

Secondly, the step-by-step compliance program, presents a structured blueprint, equipping businesses with a practical framework to methodically plan and deploy measures to adhere to these upcoming obligations. By integrating this program with their operations, businesses can actively safeguard against potential liabilities, cultivating a reputation for responsible AI deployment and ethical conduct.

Securiti's deep institutional knowledge of helping global businesses comply with the complex regulatory environment of privacy laws and regulations through the use of award winning AI powered technology makes us the best placed to provide a helping hand to AI developers and users looking for guidance today. Request a demo today and learn more about how Securiti can help your business to continue to develop and innovate using artificial intelligence without having to fear liabilities and regulatory risks.

Build Users' Trust With The Responsible Use Of GenAI