# AISWITCH AI PRACTICE COOKBOOK: EVOLVING AI-AUTONOMOUS AUTOMATION STANDARDS 2020-2021

Who should read this: Enterprise AI CoE leaders, CDO, CIO, CEO (for strategic AI initiatives), AI Business User Leaders, AI Solutions & Service Providers

Why the need to know of evolving AI standards?

2020 surveys show that more than 90% business organizations have either already implemented or are planning to implement and productionize several AI-automation solutions in their business processes and functions. This unprecedented proliferation of AI and data usage for intelligent applications and operations in the enterprises, demand strong investments in regulatory compliance of data usage and governance of AI usecases.

Consequently, not just the AI CoE leaders but the business and functional leaders who are spearheading AI initiatives in their CXO and leadership roles, must be aware of the evolving standards and regulations that will come to govern AI solutions across sectors. In some sectors such as BFSI and governments, these standards are already in force, e.g. data governance standards like GDPR, the Patriot Act, PCI-DSS and HIPAA standards, and government-specific AI policies (covered in aiswitch.org blogs- https://aiswitch.org/blogs-1#261f6ba6-4e56-4cbc-b8d9-22768d287958)
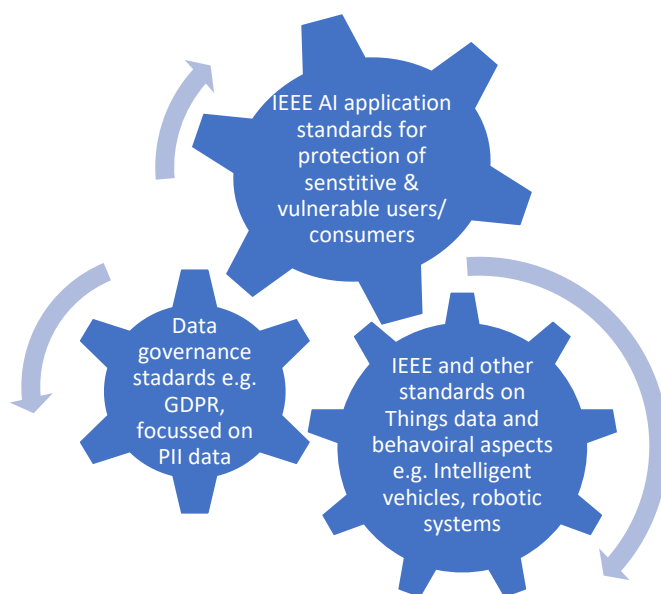
Figure 1- AI standards – Apps, Data governance, Things, Behavior

What are the most prevalent existing and evolving standards?

Some of the existing legal standards governing artificial intelligence are:

- IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems-
- The IEEE Standards Association has the IEEE P7000 series of working groups, in AI standards, comprising of 14 groups, IEEE P7001, IEEE P7002, IEEE P7002, IEEE P7003, IEEE P7004, IEEE P7005, IEEE P7006, IEEE P7007, IEEE P7008, IEEE P7009, IEEE P7010, IEEE P7011, IEEE P7012, IEEE P7013, IEEE P7014 to address issues at the meeting point of technological and ethical concerns.
- European Union's General Data Protection Regulation (GDPR)

These ethical standards and regulations range over a number of ethical concerns and are used to monitor a number of potential risks across sectors

- With a mission to deploy technological advancements for the benefit of all humanity by aiming to educate, train and empower all stakeholders involved in the design and development of autonomous and involved artificial intelligence systems, the IEEE Global Initiative is broad system of standards to build a world powered by characterized by equal access to ethical technology.

- Regulating Organizations- IEEE Draft Model Process for Addressing Ethical Concerns during System Design (IEEE P7000) and Standard for Transparent Employer Data Governance (IEEE P7005) involve the ethical considerations and human rights issues to be factored in by organizations in concept exploration and development and transparency procedures to be followed by employers in collecting, storing and using employee data respectively.

- Rights of Minors- The Standard for Child and Student Data Governance (IEEE P7004) monitors the security of data collected from students and children in terms of regulating the organizations collected this data and the permitted use of this information

- Individual Privacy Rights- Standard for Personal Data Artificial Intelligence (AI) Agent (IEEE P7006) and Data Privacy Process(IEEE P7002) regulates the technical elements used to gain access to and use personal data of individuals and the privacy rules for the same.

- Use of Robotic Systems- The Ontological Standards for Ethically Driven Robots and Systems (IEEE P7007) and Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems (IEEE P7008) oversee the incorporation of ethically driven methodologies into robotic systems and ethically driven nudging for robotic technologies.

- Put into effect in 2018, the GDPR levies strict penalties on those violating norms set for maintaining data privacy. Ranging from fairness, accuracy and transparency of the data collected, to limitations set on the amount, purpose and

storage of personal data collected, the GDPR seeks to integrate confidentiality and accountability into the entire data collection process.

How to make these standards really work in an organization? How to put them in action?

Discussing globally evolving ethical standards must also involve exploring emerging artificial intelligence technologies being developed and deployed by global organizations. Regulation need to take into account what exactly needs to be regulated, hence any discussion around ethical and legal standards of AI is incomplete without discussing globally evolving use-cases of AI, and most importantly, the rapidly emerging use of AI by global organizations, since the scale of these technologies ensures that they have the greatest impact. Just having the standards documented somewhere in the organization's repository of numerous policy documents, will clearly not work for AI usecases that are alive and kicking in a production environment.

- **Expand the scope of the standards beyond technology & data:** Policies are just as good as their executors. Current standards on GDPR and IEEE capture the data and technology governance aspects reasonably well, with 3000+ articles and artefacts related to various generic to specific AI usecases, e.g. general usage of transactional data to train AI fraud detection models, to specific policies related to decisions and actions taken by autonomous vehicles (e.g. the Perambulator problem). While technology governance standards are important, they will work if and only if they are executed in conjunction with people, process and business governance systems and practices. The scope of technology standards must be broadened to include these aspects e.g. training & awareness building on AI standards, risk measurement processes, ESG, green AI tech-stack policies.

- **Build AI-powered autonomous systems to enforce and audit standards on the actual behavior, decisions and actions of autonomous systems on ground**: Humans monitoring and auditing for standards enforced in autonomous systems beats the entire purpose of having either the systems or the standards in the first place. This is because of the fact that the speed of these systems is their key virtue, which is how they beat the latency of human decisions & actions. Only autonomous systems have the speed and accuracy of predictions and actions that can monitor, prevent and/or control damages caused by an autonomous AI system's potential violation of any standards.

123 Action items for Monday Morning

Key actions	Key actors
1-Identify and run awareness programs for all applicable AI-automation standards for AI CoE team & AI architects	AI CoE leaders, AI governance councils/ steering committee
2- Assess regulatory requirements and subsequent non-compliance risks & liabilities of all major AI initiatives	AI CoE team, chief compliance office, Chief risk office
3- Establish AI-powered self-audit systems basis standards	AI-IoT CoE tech teams,solution architects

For further information on techniques and systems: admin@aiswitch.org