Digital Policy Alert

Data Governance in International AI Frameworks

Nils Deeg

November 2026

An initiative of the
St.Gallen Endowment
for Prosperity through Trade

Data Governance in International AI Frameworks

Our text-level analysis of nine international AI frameworks shows that data governance is a universal concern across all nine frameworks. A total of 26 provisions address data governance, with various degrees of focus and actionability.

- 13 provisions focus on data governance as the core concern, while 13 provisions only touch upon data governance tangentially.
- 20 provisions across seven frameworks provide actionable measures to pursue data governance. Only 6 provisions address data governance in non-actionable language: two in the OECD AI Principles and one each in the Council of Europe Framework Convention, the G7 Code of Conduct, the UNESCO Recommendation and the UN General Assembly resolution. In the OECD Principles and the Council of Europe Framework Convention, data governance appears only in non-actionable language.
- The ASEAN Guide, UNESCO Recommendation, G7 Code of Conduct, and Joint Declaration have the most provisions on data governance, with four provisions each. In both the ASEAN Guide and the Joint Declaration, all provisions are also actionable. The frameworks with the most core provisions are the ASEAN Guide, UNESCO Recommendation, Joint Declaration, ASEAN Expanded Guide, and the UN General Assembly resolution (2 each).

We now outline the prevalence, focus, and actionability of relevant provisions in each international framework, before summarising their language.

OECD AI Principles

Two OECD AI Principles address data governance. Principle 1.2 (Respect for the rule of law, human rights and democratic values, including fairness and privacy) and Principle 1.5 (Accountability) both cover it tangentially, and neither is actionable.

- Principle 1.2 names privacy and data protection only as one of many values AI actors should respect (a).
- Principle 1.5 names privacy only as one category of risk to manage (c). Section (b) also mentions the importance of traceability with regard to datasets, though we consider this primarily a transparency measure.

UN General Assembly resolution

Two provisions in the UN General Assembly resolution A/RES/78/265 feature data governance as a core concern. One of the two is actionable. Both are framed as encouragement to Member States and, where applicable, other stakeholders.

Sub-paragraph 6(e) is actionable. Its data governance component is the development and implementation of mechanisms for securing data, including personal data protection and privacy policies. These sit alongside risk monitoring and management mechanisms and impact assessments, which are covered in the safety section.

Sub-paragraph 6(j) has data governance as its core concern but is non-actionable. It calls for safeguarding privacy and the protection of personal data when testing and evaluating systems and in transparency and reporting requirements, without identifying any specific data governance measure.

Council of Europe Framework Convention

A single article of the Convention, Article 11, is about data governance. The article is core and non-actionable. The Convention is the only instrument examined that contains "shall" obligations. These bind Parties rather than AI actors directly.

Article 11, on privacy and personal data protection, requires Parties to ensure that privacy rights and personal data are protected, including through applicable laws, standards and frameworks ((a)), and that "effective guarantees and safeguards" are in place for individuals ((b)). It does not identify any specific measure and is therefore non-actionable.

G7 Hiroshima Process Guiding Principles

Three principles feature data governance. It is the core concern of one and tangential to two. All three are actionable. The Principles are voluntary and addressed to organisations developing advanced AI systems.

Principle 11, on data input measures and protections for personal data and intellectual property, has data governance as its core concern. It suggests measures to manage data quality, including training data and data collection, to mitigate harmful biases.

Data governance is tangential to two further principles:

- Principle 5, on governance and risk management policies, encourages the disclosure of privacy policies covering personal data, user prompts and system outputs.
- Principle 6, on security controls, states that security measures taken by actors could include securing datasets.

G7 Hiroshima Process Code of Conduct

The Code of Conduct builds on the G7 Principles, adding detail in several cases. Four provisions address data governance, which is the core concern of one and tangential to three. Three of the four are actionable. For the three provisions it shares with the Principles, the Code's relevance and actionability tags are identical.

Core Provision 11 provides further detail by mentioning the possibility of employing privacy-preserving training techniques, and testing and fine-tuning to ensure that systems do not divulge confidential or sensitive data. It also adds safeguards to respect privacy rights. The risk of systems disclosing personal data is also addressed in the ASEAN Expanded Guide's Section 1.3.

Tangential provisions 5 and 6 reproduce the Principles' data governance elements, namely privacy policies and the securing of datasets.

One provision contains a data governance element with no tagged counterpart in the Principles. Provision 1, on risk identification and testing, is tangential and non-actionable: violations of privacy and data protection appear as possible risks to which testing should attend.

ASEAN Guide on AI Governance and Ethics

Four provisions in the ASEAN Guide feature data governance. It is the core concern of two provisions and tangential to two. All four provisions contain an actionable data governance element. The Guide is addressed to deployers and developers and offers worked examples and named techniques.

Two provisions take data governance as their core concern:

- Principle 5, on privacy and data governance, suggests protocols governing who can access data and when. It calls for data to be collected, stored, generated and deleted in compliance with data protection laws, and lists six national data protection laws in ASEAN. It also suggests consent or another legal basis before personal data is collected, used or disclosed, and not gathering unnecessary or irrelevant data. It recommends data protection and governance frameworks, data protection impact assessments (noting that these are narrower than an AI risk assessment) and privacy by design. It is the only provision in the dataset to name specific privacy-enhancing technologies, namely differential privacy and zero-knowledge proofs.
- The guidance on data collection and processing covers representative datasets, guidelines and quality assurance for data labelling, and five factors affecting data quality. It also covers a data provenance record, storage standards and retention policies, and encryption, access controls and anonymisation. Further, it suggests data protection impact assessments, compatibility of data use with its intended purpose, and minimising sensitive or personal data in development datasets. Developers and deployers should "reasonably avoid" using protected characteristics such as gender or ethnicity to drive decisions, while using them to assess outcomes for bias. It is the only provision in the dataset to call for due diligence on third-party sources of personal data.

In the two tangential provisions, data governance serves other principles:

- Principle 2, on fairness and equity, suggests diverse and representative training datasets and bias mitigation during data collection and pre-processing.
- Section 4, on stakeholder interaction and communication, suggests informing users and obtaining their informed consent before using their data for training, and safeguarding the security of user data. It also suggests feedback channels through which users can correct inaccurate personal data. It is the only provision in the dataset that provides for the correction of personal data.

ASEAN Expanded Guide on AI Governance and Ethics – Generative AI

The Expanded Guide on Generative AI builds on the 2024 Guide, adapting its underlying principles to the generative AI context. Two provisions are about data governance as a core concern. Both are actionable.

Section 1.3 restates the seven principles of the 2024 Guide, reproducing its definition of privacy and data governance. The new elements specific to generative AI address the scraping of internet data and the risk that models "memorise" and release training data. To meet these, the section suggests data minimisation and anonymisation, safeguards within the model to refuse to disclose personal data, and a legal basis such as consent. It also suggests data traceability and internal verification of data accuracy and integrity. Under its security principle, it adds secure data collection and storage, a response plan for data breaches and safeguards against data poisoning.

Section 3.2, on data, takes data governance as its core concern. It notes that internet-sourced training data requires attention to usage rights, provenance, accuracy and personal data protection. As areas for ASEAN to explore, it proposes a common regional approach to personal data protection and regional guidelines on data handling, storage and governance. It also proposes measurable regional benchmarks on data quality and guidance on cross-border data flows related to AI. Its proposals are directed at ASEAN as a convening body rather than at organisations. Its material on data sharing and regional language models is unrelated.

UNESCO Recommendation on the Ethics of AI

Four provisions are related to data governance, of which two are core and a further two tangential. Three of the four are actionable.

Two provisions take data governance as their core concern:

- The principle 'Right to privacy, and data protection' (paragraphs 32 to 34) calls for data to be collected, used, shared, archived and deleted consistently with international law (paragraph 32). It calls for data protection frameworks requiring a legitimate aim and a valid legal basis, including informed consent, and for data subjects to be able to exercise their rights (paragraph 33). It also calls for privacy impact assessments and privacy by design (paragraph 34).
- Policy Area 3, on data policy, is addressed to Member States. It calls for data governance strategies that continually evaluate the quality of training data and ensure data security (paragraph 71), and for privacy impact assessments and privacy by design (paragraph 72). It calls for a framework giving individuals rights over their personal data, including the ability to access and erase it, safeguards for sensitive data, and protection where data are used for micro-targeted advertising or transferred across borders (paragraph 73). It further calls for full security for sensitive data such as biometric, genetic and health data (paragraph 74), and for quality datasets built on a valid legal basis with annotation standards (paragraph 76).

In the two tangential provisions, data governance serves other objectives:

- Policy Area 11, on health and social well-being, calls for compliance with data protection requirements in health AI (paragraph 123(c)). It also calls for informed consent to the use and analysis of personal data without preventing access to health care (paragraph 123(d)).
- The principle 'Safety and security' (paragraph 27) names privacy-protective data access frameworks and quality training data only as enablers of safe AI, and is therefore non-actionable.

Joint Declaration on AI, Freedom of Expression and Media Freedom

Four provisions in the Joint Declaration are relevant to data governance. Two are core provisions and two are tangential. All four are actionable. The Declaration addresses states, companies, financial institutions and investors, as well as journalists and media actors.

Data governance is a core concern of Principle 3, on respecting privacy and data protection. Its actionable component is the call to respect international data protection standards throughout the lifecycle, "including consent, purpose limitation".

The section on state regulation of companies is also core. Its data governance component calls for strong data protection laws that enable transparency in data collection and use ((c)). These laws should limit "extractive data mining practices" and pervasive tracking and targeting of individuals online, and ensure that data extraction for AI training is based on consent. The section's other material on due diligence, oversight institutions, competition and linguistic diversity is unrelated.

In the two tangential provisions, data governance serves other objectives:

- The section addressed to the private sector calls on companies to develop and train AI systems in full respect of data protection ((d)), to develop standards for fair data extraction ((e)), and to adopt clear privacy and data protection policies ((g)).
- The section on journalists and media actors calls on them, when choosing an AI provider, to rigorously evaluate the diversity, fairness and quality of its data and its compliance with privacy and data protection ((c)).

Digital Policy Alert

Contact
Written by Nils Deeg
Please send questions and suggestions to nils.deeg@sgept.org

The independent Digital Policy Alert is a pillar of the Swiss-based
St. Gallen Endowment for Prosperity Through Trade

St.Gallen Endowment
for Prosperity through Trade