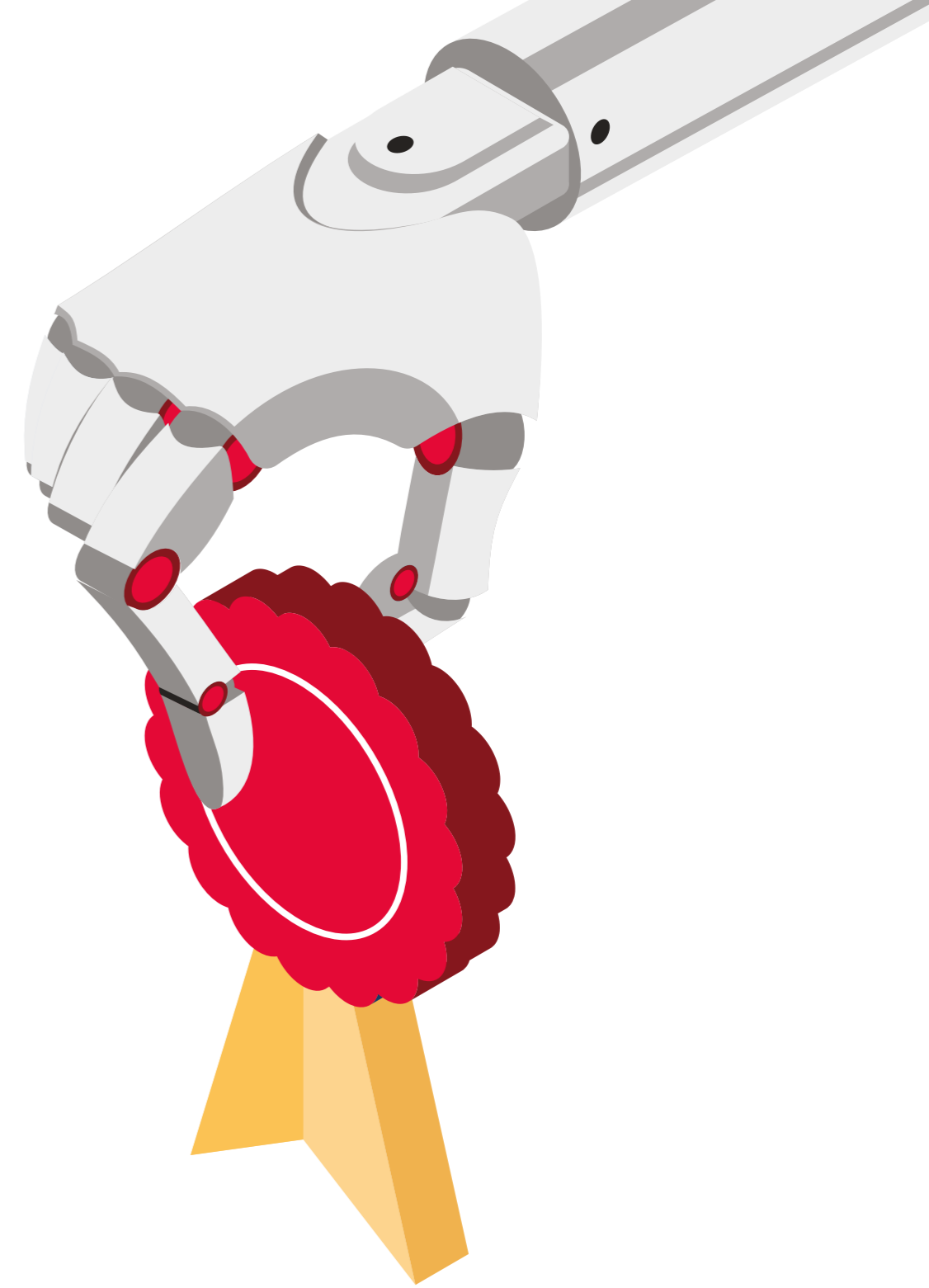




Generative AI Contract Best Practice

Mitigating risks and driving responsible use
of Gen AI across the marketing supply chain



Contents

Introduction

Contract compliance: the cornerstone to responsible generative AI

3

Generative AI considerations

Issues that marketers may want to address in contracts

4

What makes a robust contractual clause?

8

Nine steps to ensuring contract compliance

9

Annex

Regulations impacting the use of generative AI in key markets

12



Contract compliance: the cornerstone to responsible generative AI

Contract compliance is a cornerstone of marketing best practice, essential to ensuring that brands and agencies meet legal and ethical obligations and mitigate risk.

When using generative AI (gen AI), this becomes even more critical due to the technology's potential to produce outputs which inadvertently violate company terms, intellectual property, privacy, confidentiality or national laws and regulations. For a more comprehensive overview of the opportunities and challenges of generative AI, see [WFA's Generative AI Primer](#).

WFA research of the world's largest brands finds that legal, ethical and reputational risks continue to be the main barriers to generative AI adoption. That's why over 50% are now putting in place responsible AI policies to guide their organisations' use of the technology and mitigate risks.

However, much risk lies outside of marketers' direct control, and 80% of brands are concerned about how partners are using generative AI on their behalf.

As a result, 53% are planning to review their contracts with partners, including agencies and vendors, to ensure responsible use and governance of gen AI across their supply chain.

This document, developed in partnership with marketing consultancy R3, seeks to assist marketers' contract reviews to increase transparency and trust in gen AI adoption and safeguard brand reputation.

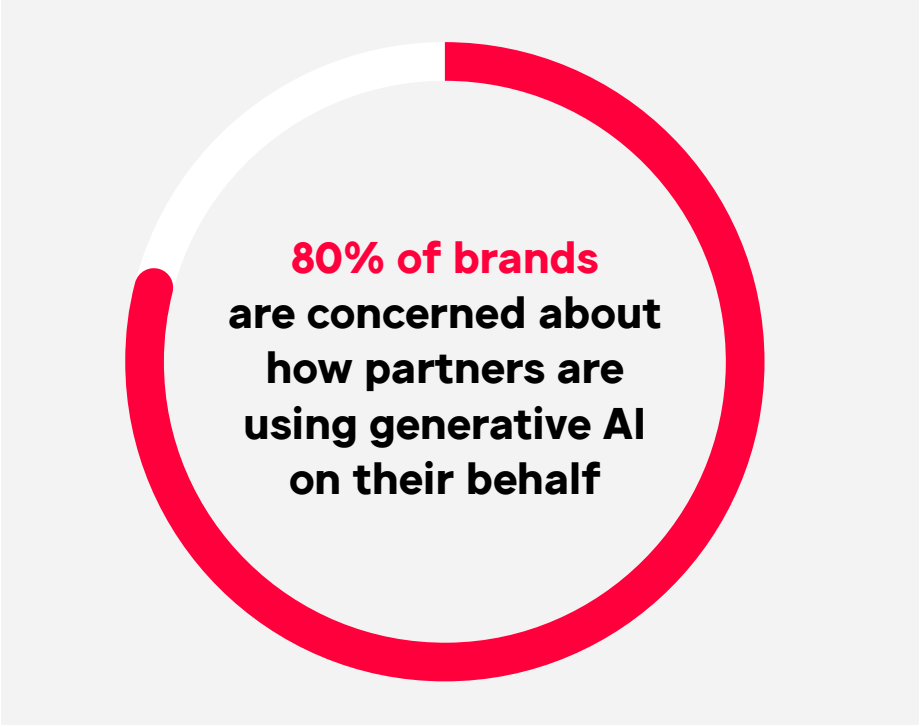
In particular, it seeks to:

- 1 Provide insights into the types of gen AI issues that could be addressed in contracts.
- 2 Explore what makes a robust contractual clause.
- 3 Share practical steps to drive gen AI contract compliance with agencies and vendors.
- 4 Drive awareness of variations in regulation impacting the use of generative AI across key markets globally.

We believe incorporating such considerations into contract terms can help brands by providing a clear framework for the use, deployment and control of gen AI technologies for marketing purposes. This could be crucial to maximising the benefits of gen AI while mitigating risks.

The information provided in this document is for the purposes of education and awareness and does not constitute legal advice.

The rapid evolution of generative AI and its application and governance means that the content of this document can only be accurate at its time of production. We will endeavour to update this document annually and welcome feedback.



**80% of brands
are concerned about
how partners are
using generative AI
on their behalf**

Gen AI considerations in contract compliance

Issues that marketers may want to address in contracts

Data Privacy & Security

- **GDPR and Other Data Protection Laws:** Marketers should seek to ensure that any personal data collected and used by agencies or vendors complies with relevant data protection regulations, such as the EU GDPR, CCPA in California, or other regional laws. Contracts should aim to specify how data will be collected, processed, and stored.
- **Personal data security:** If personal data is involved, contracts should stipulate certain technical and organizational measures to ensure a level of personal data security (e.g. pseudonymization or anonymization).
- **Data Ownership and Usage Rights:** Contracts should seek to clarify who owns the data used and generated by AI. Contracts should define usage rights, ensuring that data used for AI training is lawfully collected and used.
- **Data security protocols:** Contracts should ensure that gen AI tools being used have appropriate security measures in place to protect the brand information being used to prompt models and generate outputs.

These efforts help ensure that advertisers are protected in case of data misuse, that their data is adequately safeguarded and that roles and responsibilities for compliance with relevant legislation are clear.

Intellectual Property (IP)

- **Rights over data inputs:** Contracts should ensure clear obligations on providers to secure the necessary rights to use brand IP for generating outputs. Brands should also consider seeking clarity as to how such company IP may be used for further purposes (e.g. model training).
- **Ownership of AI-Generated Content:** Contracts should aim to clearly outline who owns the content generated by AI and how it can be used. This is crucial for avoiding disputes over the rights to use, distribute, or modify AI-generated works. In agency contracts, it may be important to clarify that any rights obtained by the agency for outputs should be transferred to the brand.
- **Record keeping:** Contracts should ensure clear guidance on the types of documentation and records that need to be kept to demonstrate company confidentiality was upheld, to support ownership claims or to respond to potential IP infringement allegations. Such records could include details on information input into the tool, prompts used to generate outputs and any outputs.
- **Indemnities and warranties:** Contracts should ensure that any third-party content used to generate outputs or train generative AI models is legally obtained and licensed. Contracts should also include warranties about the legality of their data sources.

These efforts will help brands ensure that their own company IP is adequately protected when being used to prompt generative AI models, that there is clarity over who owns outputs, and adequate protections in case of IP infringement claims.

Gen AI considerations in contract compliance

Issues that marketers may want to address in contracts

Ethical & Responsible Use

- **Bias and Fairness:** Contracts should consider addressing the need for AI systems to be designed and used in a manner that avoids bias and ensures fairness. This may include requiring gen AI providers to conduct bias testing, adopt measures to ensure fairness and provide transparency in AI decision-making.
- **Transparency Requirements:** Contracts should ideally require AI providers to meet transparency standards and introduce clear processes for when and how agencies should disclose to brands when gen AI has been used in deliverables.
- **Algorithmic transparency:** Marketers may want to seek to ensure that generative AI providers are transparent about how models were built, their algorithms work and how decisions are taken so that they can more accurately explain these decisions and outcomes to regulators or consumers.
- **Responsible AI:** Contracts should ensure that any responsible AI policies and principles adopted by brands (e.g. which stipulate acceptable and unacceptable use cases or tools) are transferred to and adhered by partners.

These efforts will help brands ensure that their own commitments to diversity, equity and inclusion, transparency and responsible AI are adhered to by gen AI providers or partners.

Liability & Risk Management

- **Definition of AI:** All parties will benefit from having a shared understanding of what is meant by “generative AI”. This includes the specific technologies, methods, or systems that are covered under the agreement.
- **Liability for AI outputs:** Contracts should look to clearly define who is responsible if the generative AI system generates content or outputs that infringe on intellectual property, violates laws, or causes harm. This includes specifying indemnification clauses to protect against potential legal actions.
- **Product and Service Warranties:** Marketers may want to require AI providers to offer warranties regarding the accuracy, reliability, and legality of the AI system’s output.
- **Limitation of Liability:** Contracts should include clauses that limit the marketer’s liability for unintended consequences of AI-generated content, especially when the AI system is provided by a third-party vendor.

These efforts help marketers define the scope of generative AI usage, clarify responsibilities in case of harmful or unlawful AI outputs and set expectations for accuracy and legality through warranties. They also protect companies from excessive liability.



Gen AI considerations in contract compliance

Issues that marketers may want to address in contracts

Regulatory Compliance

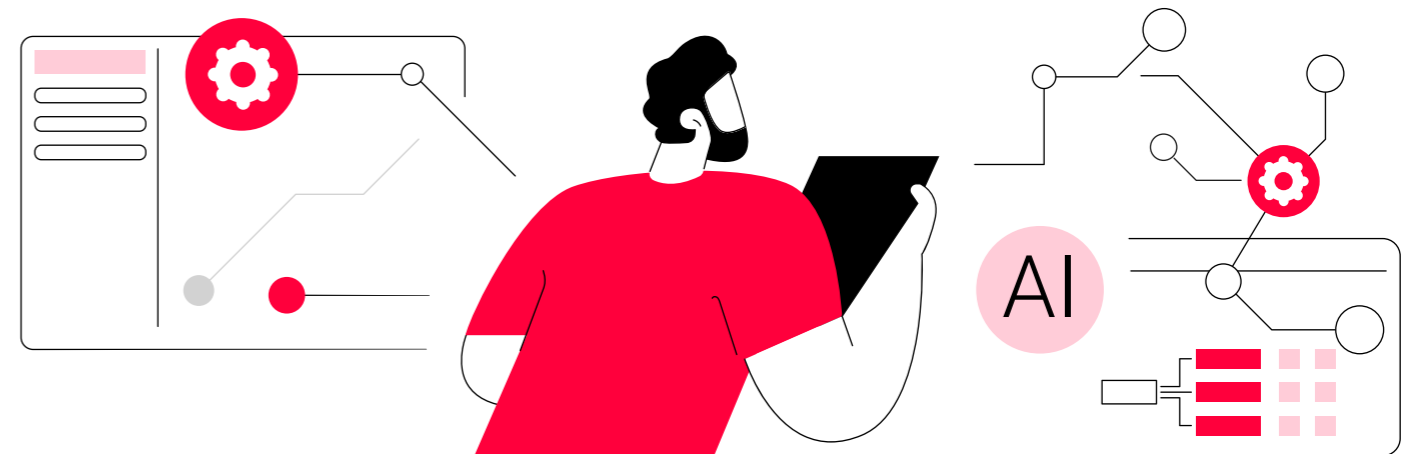
- **Adherence to Advertising Standards:** Contracts should ensure that AI-generated content complies with industry-specific advertising regulations, such as those governing truth in advertising, endorsements, and marketing to children.
- **Consumer Protection:** Contracts must ensure that the AI use complies with consumer protection laws, preventing deceptive practices and ensuring that AI-generated content does not mislead or harm consumers.
- **Compliance with AI-Specific or AI-related Regulations:** Be aware of emerging AI regulations, such as the proposed EU AI Act, and include contractual obligations to comply with these regulations as they become law.
- **Cross-Border Data Transfers:** If generative AI involves cross-border data transfers, contracts should address compliance with international data transfer regulations, including the use of standard contractual clauses (SCCs) or other legal mechanisms.

These efforts help brands ensure that generative AI use adheres to advertising, consumer protection and other laws and self-regulation, prevent deceptive practices and maintain consumer protection.

Service-Level Agreements (SLAs) & Performance Metrics

- **AI System Performance:** Contracts should specify performance metrics for AI systems, such as accuracy, reliability, and uptime. SLAs should include remedies for underperformance, such as service credits or penalties.
- **Maintenance and Updates:** Brands should seek to ensure that the AI provider is contractually obligated to maintain and update the AI system to keep it compliant with evolving laws and standards.

These efforts help brands ensure that partners and AI systems are taking necessary steps to meet specified performance standards and comply with evolving laws and standards.



Gen AI considerations in contract compliance

Issues that marketers may want to address in contracts

Termination Clauses

- **Termination for Breach:** Marketers should include clear terms for contract termination in case of non-compliance with the agreed-upon standards, especially related to data protection, IP rights, and ethical use.
- **Data Retrieval and Deletion:** Upon contract termination, marketers should ensure that any data provided or generated is either returned or securely deleted, with contractual assurances from the AI provider.

These efforts will help brands ensure that there is clarity on how to disengage from AI providers and partners and how data and information is handled upon contract termination to protect any proprietary information.

Dispute Resolution

- **Arbitration and Jurisdiction:** Contracts should include dispute resolution mechanisms, such as arbitration or specifying the jurisdiction for legal disputes, to address any issues that arise from the use of generative AI.

These efforts will help brands develop a roadmap for handling any potential conflicts, offering a measure of predictability and control in uncertain situations. This will enable brands to make more informed decisions, allocate risk more effectively, and approach disagreements in good faith.

Audit Rights & Monitoring

- **Right to Audit:** Contracts should grant marketers the right to audit AI systems to ensure compliance with contractual obligations, particularly regarding data protection and ethical use. It should also specify where and how these audits are undertaken.
- **Ongoing Monitoring:** Establish provisions for continuous monitoring of AI outputs to ensure ongoing compliance with legal and ethical standards.

These efforts help ensure brands have sufficient auditing rights so that they can identify and address any compliance or performance issues and ensure generative AI tools being used remain effective.

Training & Awareness

- **Staff Training:** Marketers should ensure that their teams, including those of their partners, are trained on the legal and ethical implications of using generative AI, including understanding the contract terms and compliance obligations.
- **AI Provider/Partner Support:** Include contractual commitments from AI providers to offer support and training on the responsible use of their AI systems.

These efforts help ensure that brands' own responsible AI efforts are being adopted by partners using generative AI on their behalf and avoid misuse of AI capabilities.

What makes a robust AI disclosure clause?

Considerations

Start with “why”

Understanding the main reason behind what you’re going to protect yourself from will dictate how the clause is drafted.

Define AI

How do you define the term “artificial intelligence” to ensure that all parties are clear on the scope of the disclosure requirement.

What’s the purpose of using AI?

The purpose of using AI can activate certain legal obligations in specific markets. The EU’s AI Act outlines use cases where AI use is prohibited.

Indicate the AI types the vendor will use

Provide examples of the AI types the vendor must disclosed, i.e. facial recognition, predictive analytics. AI types might activate a general or specific law, and being specific will help with compliance.

Create an obligation to disclose the use of AI

Specify that the vendor must make this disclosure to you.

State when disclosure must take place

Specifying if the disclosure must be done before certain milestones are started within the process will ensure that not only that work is created that complies with law, but it is work you have paid for that is cleared for use.

State the form in how disclosure must be received

Specific if this must be in a certain medium (i.e., email) and that receipt of the email must be confirmed by a certain individual or team.

Explain limits and biases

Vendor should highlight any potential biases in the system. For instance, you may want the vendor to comply with an international standard on preventing bias, like ISO/IEC TR 24027:2021.

Key steps to consider to ensure Gen AI contract compliance

1 Understand the Legal and Regulatory Framework

- **Identify Relevant Laws:** Determine which laws and regulations apply to the use of generative AI, including data protection laws (e.g., GDPR, CCPA), intellectual property laws, and sector-specific regulations (e.g., healthcare, finance).
- **Stay Updated on Changes:** Regularly monitor legal developments related to AI, as regulations are evolving rapidly. This includes keeping an eye on proposed laws, such as the EU AI Act or Canada's AIDA, that may impact AI use.

2 Review and Draft AI Contracts Carefully

- **Define Scope of Use:** Clearly outline how generative AI will be used, including the specific purposes, the data involved, and any limitations on its use.
- **Include Data Protection Clauses:** Ensure contracts include robust data protection provisions that comply with relevant laws. This includes clauses on data ownership, data minimization, data security, and the rights of data subjects.
- **Address Intellectual Property (IP) Rights:** Clearly define the ownership of AI-generated content, the use of training data, and any licensing agreements. Ensure that the contract specifies who holds the IP rights to AI outputs and any restrictions on their use.
- **Incorporate Ethical and Compliance Standards:** Embed ethical AI guidelines and compliance requirements into contracts. This could include commitments to transparency, non-discrimination, and accountability in AI use.

3 Conduct Due Diligence on AI Vendors and Partners

- **Vendor Assessments:** If using third-party AI vendors, assess their compliance with relevant laws and their adherence to ethical standards. This includes evaluating their data handling practices, security measures, and transparency about AI models.
- **Third-Party Compliance:** Ensure that all partners involved in the AI supply chain, including data providers, cloud services, and AI developers, comply with contractual obligations and legal requirements.



Key steps to consider to ensure Gen AI contract compliance

4 Implement Data Governance Practices

- **Data Inventory and Classification:** Maintain a comprehensive inventory of all data used by generative AI systems, including personal data, proprietary data, and third-party data. Classify the data based on sensitivity and legal requirements.
- **Data Minimization:** Collect and use only the data necessary for the specific AI application. Ensure that data processing aligns with the principles of purpose limitation and data minimization.
- **Data Subject Rights Management:** Implement processes to manage requests related to data subject rights, such as access, correction, deletion, and opt-out requests, in compliance with applicable laws like GDPR and CCPA.

5 Monitor AI System Performance and Compliance

- **Regular Audits and Assessments:** Conduct regular audits of AI systems to ensure they are functioning as intended and complying with contractual and legal obligations. This includes checking for biases, data protection issues, and IP compliance.
- **Risk Management:** Identify and mitigate risks associated with generative AI, such as privacy risks, ethical concerns, and potential for IP infringement. Develop risk management strategies that address these issues proactively.

6 Train Employees and Stakeholders

- **Awareness and Training Programs:** Educate employees, particularly those involved in AI development and deployment, about the legal, ethical, and compliance aspects of generative AI. Ensure they understand their roles in maintaining compliance.
- **Ethical AI Practices:** Promote a culture of ethical AI use within the organization. This includes training on the responsible use of AI, understanding biases, and recognizing the implications of AI decisions on individuals and society.



Key steps to consider to ensure Gen AI contract compliance

7 Document and Communicate Compliance Efforts

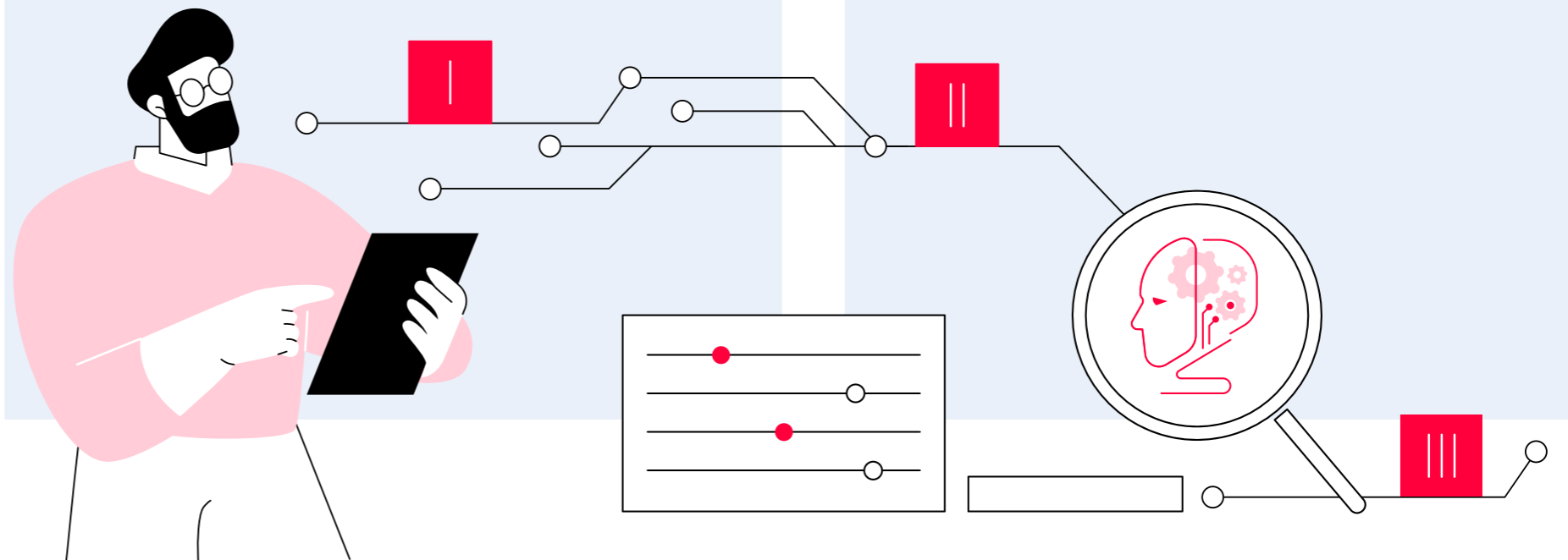
- **Maintain Documentation:** Keep detailed records of all compliance activities, including contracts, data processing agreements, audit results, and risk assessments. This documentation is crucial in case of regulatory scrutiny or legal disputes.
- **Transparent Communication:** Communicate your AI compliance efforts to stakeholders, including customers, regulators, and partners. Transparency can build trust and demonstrate your commitment to responsible AI use.

8 Engage Legal and Compliance Experts

- **Consult Legal Counsel:** Regularly consult with legal experts to ensure that your use of generative AI complies with the latest laws and regulations. Legal counsel can help in drafting contracts, assessing risks, and addressing complex compliance issues.
- **Compliance Officers:** Appoint or consult with compliance officers who specialize in AI, data protection, and technology law. They can oversee compliance efforts and ensure that the organization adheres to all relevant obligations.





9 Prepare for Dispute Resolution

- **Awareness and Training Programs:** Include Dispute Resolution Clauses: Ensure that contracts involving generative AI include clear dispute resolution mechanisms, such as arbitration or mediation, to address any disagreements related to AI use.



Best practice: North America

Existing Gen AI regulation

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Canada</p>		<p>Personal Information Protection and Electronic Documents Act (PIPEDA)</p> <ul style="list-style-type: none"> • Governs how private sector organizations collect, use, and disclose personal information in the course of commercial activities. Specific provinces, like Quebec, British Columbia, and Alberta have their own privacy laws which supplement PIPEDA. <p>Artificial Intelligence and Data Act (AIDA) – Proposed Legislation</p> <ul style="list-style-type: none"> • Aims to regulate high-impact AI systems and establish a framework for responsible AI use. <p>Intellectual Property Law</p> <ul style="list-style-type: none"> • Including copyright, patent, and trademark laws; also covers use of training data where generative AI models trained on copyrighted material must ensure that the use of such data does not infringe on intellectual property rights.
 <p>USA</p>		<p>California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)</p> <ul style="list-style-type: none"> • Impacts how personal data is used in AI systems, including generative AI, by granting California residents rights over their personal data, such as the right to know, delete, and opt-out of data sales. <p>Virginia (Virginia Consumer Data Protection Act), Colorado (Colorado Privacy Act), and Connecticut</p> <ul style="list-style-type: none"> • Imposes obligations on businesses that use personal data in AI systems. <p>Copyright Law</p> <ul style="list-style-type: none"> • Works generated entirely by AI without human authorship may not be eligible for copyright protection; if a human plays a significant role in the creation process, the resulting work may qualify for copyright protection. <p>Patent Law</p> <ul style="list-style-type: none"> • Current law requires that inventors be human, which has implications for patents involving AI-generated inventions. <p>Equal Employment Opportunity Laws</p> <ul style="list-style-type: none"> • Laws prohibit discrimination based on race, gender, disability, age, and other protected characteristics.

AI related regulation: CCPA

The California Consumer Privacy Act (CCPA) has significant implications for the use of generative AI, particularly regarding how personal data is collected, processed, and utilized.

1. Data Collection and Use Implications for Generative AI:

- **Transparency and Disclosure:** Under the CCPA, businesses must inform consumers about what personal data is being collected and how it will be used. If a generative AI system uses personal data for training or content generation, businesses must disclose this to consumers. This transparency requirement means that businesses need to clearly explain how generative AI systems handle personal data.
- **Purpose Limitation:** Businesses are required to specify the purposes for which personal data is collected. If personal data is used to train generative AI models, this purpose must be explicitly communicated to the consumer. This limits the use of data to what consumers have been informed about and consented to.

2. Consumer Rights Implications for Generative AI:

- **Right to Opt-Out:** The CCPA gives consumers the right to opt-out of the sale of their personal information. If a generative AI system involves the sale or sharing of personal data, businesses must provide a mechanism for consumers to opt-out. This could impact the datasets available for training generative AI models, as consumers may choose to restrict the use of their data.
- **Right to Access:** Consumers have the right to request access to the personal information collected about them. For generative AI, this means that businesses must be able to provide details about what personal data has been used in AI models or outputs related to the consumer.
- **Right to Deletion:** Consumers can request the deletion of their personal data under the CCPA. If a generative AI system has used personal data, businesses may be required to delete that data, which could also include removing data from AI training sets or retraining models to exclude that data.

3. Data Minimization and Security Implications for Generative AI:

- **Data Minimization:** The CCPA encourages businesses to collect only the personal information that is necessary for the specific purpose disclosed to the consumer. For generative AI, this implies that companies should limit the amount of personal data used in AI training models to what is strictly necessary, reducing the risk of over-collection.
- **Security Obligations:** The CCPA mandates that businesses implement reasonable security measures to protect personal data. This requirement extends to generative AI systems, where businesses must ensure that any personal data used in AI models is securely stored and protected against unauthorized access or breaches.

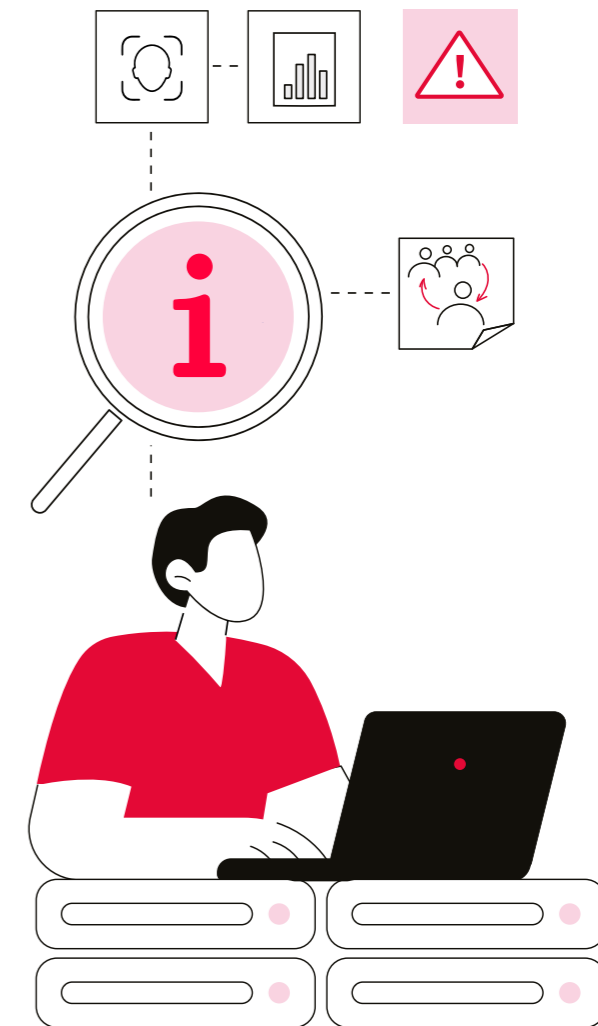
AI related regulation: CCPA (Continued)

4. Profiling and Automated Decision-Making Implications for Generative AI:





- **Profiling Concerns:** Generative AI can be used to create profiles of individuals or generate content based on personal data. The CCPA does not specifically regulate automated decision-making or profiling, but it does empower consumers to understand and control how their personal information is used. Businesses using generative AI for profiling must consider these rights and ensure that consumers are aware of and consent to such uses.
- **Potential Future Regulation:** As discussions around AI regulation continue, it is possible that future amendments to the CCPA or new legislation could address specific concerns related to AI-driven profiling and automated decision-making.

5. Penalties for Non-Compliance Implications for Generative AI:

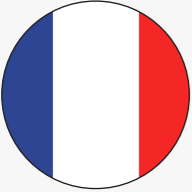



- **Legal and Financial Risks:** Non-compliance with the CCPA can result in significant fines and penalties, including statutory damages in cases of data breaches. For businesses using generative AI, failure to adhere to CCPA requirements could result in legal actions and financial liabilities, particularly if personal data is misused or inadequately protected.





AI related regulation: Europe & UK

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Czech Republic</p>		<p>General Data Protection Regulation (GDPR)</p> <ul style="list-style-type: none"> As a member of the European Union, the Czech Republic is subject to the GDPR, which governs the processing of personal data. <p>Copyright Act (Zákon č. 121/2000 Sb., Autorský zákon)</p> <ul style="list-style-type: none"> Protects the rights of creators and authors over their intellectual property. <p>Industrial Property Act (Zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích)</p> <ul style="list-style-type: none"> Governs patents, trademarks, and other forms of industrial property. <p>Consumer Protection Act (Zákon č. 634/1992 Sb., o ochraně spotřebitele)</p> <ul style="list-style-type: none"> Designed to protect consumers from unfair, misleading, or abusive business practices.
 <p>Germany</p>		<p>As an EU member, Germany is subject to the GDPR, which is one of the most stringent data protection frameworks globally.</p> <p>Copyright Act (Urheberrechtsgesetz, UrhG)</p> <ul style="list-style-type: none"> Protects the rights of creators and authors over their works. <p>Patent Law (Patentgesetz, PatG) and Trademark Law (Markengesetz, MarkenG)</p> <ul style="list-style-type: none"> Govern patents and trademarks. <p>Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb, UWG)</p> <ul style="list-style-type: none"> Protects consumers from misleading and unfair business practices.

AI related regulation: Europe & UK

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>France</p>		<p>As an EU member, France is subject to the GDPR, which is one of the most stringent data protection frameworks globally.</p> <p>French Data Protection Act (Loi Informatique et Libertés)</p> <ul style="list-style-type: none"> • Guidelines and recommendations on AI and data protection, emphasizing the need for transparency, fairness, and accountability in AI systems. <p>Intellectual Property Code (Code de la propriété intellectuelle, CPI)</p> <ul style="list-style-type: none"> • Governs copyright, patents, trademarks, and other intellectual property rights. <p>Consumer Code (Code de la consommation)</p> <ul style="list-style-type: none"> • Protects consumers from unfair, misleading, or deceptive practices. <p>Digital Republic Law (Loi pour une République numérique)</p> <ul style="list-style-type: none"> • Promotes transparency, access to data, and digital inclusion while ensuring that digital technologies, including AI, are used responsibly.
 <p>Italy</p>		<p>As an EU member, Italy is subject to the GDPR, which is one of the most stringent data protection frameworks global.</p> <p>Italian Data Protection Code</p> <ul style="list-style-type: none"> • Includes specific provisions that may impact AI, such as those related to the processing of personal data in specific sectors, including health and financial services.

AI related regulation: Europe & UK

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>UK</p>		<p>UK GDPR and Data Protection Act 2018</p> <ul style="list-style-type: none"> • Primary legal frameworks governing the use of personal data in the UK. These laws significantly impact generative AI when personal data is involved, ensuring that AI systems comply with principles such as lawfulness, fairness, transparency, data minimization, and accuracy. <p>Equality Act 2010</p> <ul style="list-style-type: none"> • Prohibits discrimination based on protected characteristics such as age, gender, race, and disability. <p>Consumer Rights Act 2015</p> <ul style="list-style-type: none"> • Influence how AI-generated content and products are presented and marketed.



AI related regulation: Europe GDPR

The EU General Data Protection Regulation (GDPR) has several key provisions that significantly impact and influence the use of generative AI, especially when such systems process personal data. Here are some relevant references that affect generative AI

1. Lawfulness, Fairness, and Transparency (Article 5(1)(a)) Impact on Generative AI:

- Generative AI systems must process personal data lawfully, fairly, and transparently. This means that organizations deploying AI must ensure that the data used is processed in a way that is understandable and does not mislead individuals. If generative AI models use personal data, organizations must clearly inform data subjects about how their data will be used, ensuring transparency in AI operations.

2. Purpose Limitation (Article 5(1)(b)) Impact on Generative AI:

- Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. This provision restricts how generative AI systems can use personal data. Organizations must ensure that the data used to train or feed into generative AI is used strictly for the purposes initially defined and cannot be repurposed without obtaining further consent.

3. Data Minimization (Article 5(1)(c)) Impact on Generative AI:

- The principle of data minimization requires that only the data necessary for the specific purpose is collected and processed. Generative AI systems must not collect excessive or irrelevant data. AI developers need to ensure that their models use only the minimum amount of personal data necessary to achieve their intended purpose.

4. Accuracy (Article 5(1)(d)) Impact on Generative AI:

- Personal data must be accurate and kept up to date. For generative AI, this means that the data used to train or inform AI models should be accurate to prevent generating misleading or incorrect outputs. If generative AI systems rely on inaccurate data, they may produce erroneous or biased outputs, leading to potential GDPR violations.

AI related regulation: Europe GDPR

(Continued)

5. Storage Limitation (Article 5(1)(e))

Impact on Generative AI:

- Personal data should be kept in a form that permits identification of data subjects for no longer than necessary. Generative AI systems must comply with this requirement by not retaining personal data indefinitely. Organizations using generative AI must implement data retention policies to ensure that personal data is deleted or anonymized when it is no longer needed.

6. Integrity and Confidentiality (Article 5(1)(f))

Impact on Generative AI:

- Personal data must be processed in a way that ensures its security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. Generative AI systems must implement robust security measures to protect personal data. This includes using encryption, access controls, and other cybersecurity measures to safeguard data within AI systems.

7. Lawful Basis for Processing (Article 6)

Impact on Generative AI:

- Organizations must have a lawful basis for processing personal data, such as consent, contract performance, legal obligation, vital interests, public tasks, or legitimate interests. For generative AI systems, obtaining explicit consent from data subjects is often the most relevant lawful basis, especially if the AI processes sensitive data or uses data for purposes beyond the original collection context.

8. Consent (Articles 7 & 8)

Impact on Generative AI:

- Consent must be freely given, specific, informed, and unambiguous. For minors, stricter rules apply. Generative AI systems that rely on personal data must ensure that valid consent is obtained from data subjects. Users must be informed clearly about how their data will be used by AI, and they must be given the option to withdraw consent at any time.

AI related regulation: Europe GDPR

(Continued)

9. Rights of the Data Subject (Articles 12-22)

Impact on Generative AI:

- The GDPR grants individuals various rights regarding their personal data, including the right to access (Article 15), rectification (Article 16), erasure (Article 17, also known as the “right to be forgotten”), restriction of processing (Article 18), data portability (Article 20), and objection (Article 21). Generative AI systems must be designed to accommodate these rights, allowing users to access, correct, or delete their data, as well as to object to or restrict data processing.

10. Automated Decision-Making, Including Profiling (Article 22)

Impact on Generative AI:

- Article 22 restricts the use of solely automated decision-making, including profiling, that produces legal effects or significantly affects individuals. Generative AI systems that might be used in automated decision-making processes must ensure that human oversight is in place. Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, unless certain conditions are met (e.g., explicit consent, necessity for a contract).

11. Data Protection by Design and by Default (Article 25)

Impact on Generative AI:

- Organizations are required to implement data protection measures at the design stage of any data processing activity, including AI systems. This means that privacy and data protection must be integrated into the design and development of generative AI systems. Generative AI must be built with privacy-preserving features, ensuring that default settings protect personal data to the greatest extent possible.

12. Data Protection Impact Assessments (DPIAs) (Article 35)

Impact on Generative AI:

- DPIAs are required when processing, including the use of AI, is likely to result in a high risk to the rights and freedoms of individuals. Generative AI systems, especially those handling sensitive data or used in high-risk applications, must undergo DPIAs. A DPIA helps identify and mitigate risks associated with data processing in AI systems, ensuring compliance with GDPR.

AI related regulation: Europe GDPR

(Continued)

13. Data Breach Notification (Articles 33 & 34) Impact on Generative AI:

- In the event of a data breach involving personal data, organizations must notify the relevant supervisory authority within 72 hours and, in certain cases, the affected data subjects. Generative AI systems must have protocols in place to detect and report data breaches promptly. This provision ensures that any breach of personal data used by generative AI is addressed swiftly, minimizing potential harm to data subjects.

14. Appointment of a Data Protection Officer (DPO) (Articles 37-39) Impact on Generative AI:

- Organizations that process large amounts of personal data, especially sensitive data, may be required to appoint a Data Protection Officer (DPO). For companies using generative AI extensively, appointing a DPO helps ensure ongoing compliance with GDPR. The DPO oversees the organization's data protection strategies, including those related to the use of AI.



AI related regulation: EU AI Act (obligations not yet applicable)

A comprehensive regulatory framework has recently been adopted by the European Commission to govern the use and development of artificial intelligence (AI) across the European Union. It aims to ensure that AI systems are safe, respect fundamental rights, and promote trustworthy AI innovation. Here are the key points of the EU AI Act:

1. Risk-Based Classification System

- **High-Risk AI Systems:** The Act categorizes AI systems based on the level of risk they pose. High-risk AI systems, such as those used in critical infrastructure, education, employment, and law enforcement, are subject to stringent requirements. These include strict data governance, transparency, human oversight, and robust risk management systems.
- **Limited-Risk AI Systems:** AI systems that interact with humans, such as chatbots, are classified as limited-risk. These systems must comply with transparency obligations, such as informing users that they are interacting with AI.
- **Minimal or Low-Risk AI Systems:** AI systems that pose minimal or low risk, like AI used in video games or spam filters, are subject to fewer regulations. The Act encourages the voluntary adoption of codes of conduct for these systems.

2. Prohibited AI Practices

The Act outright bans certain AI practices considered to be a threat to safety, rights, and democratic values.

These Include:

- AI systems that manipulate human behavior to the detriment of users (e.g., exploiting vulnerabilities of specific groups).
- AI systems used for social scoring by governments, akin to the social credit systems used in some countries.
- Real-time remote biometric identification in public spaces by law enforcement, with very limited exceptions.

WFA has developed a briefing on the EU AI Act, outlining the key provisions and potential implications for advertisers. For further information, please see [here](#).

AI related regulation: EU AI Act (obligations not yet applicable)

(Continued)

3. Transparency and Disclosure Requirements

- AI systems classified as high-risk must meet stringent transparency obligations. Users must be informed when they are interacting with AI, and the AI's capabilities and limitations must be disclosed.
- For AI systems that generate or manipulate content (e.g., deepfakes), the Act requires clear labeling to indicate that the content is AI-generated.

5. Human Oversight

- The Act mandates that high-risk AI systems must be designed to allow effective human oversight. This includes the ability to intervene in or override AI decisions when necessary.
- There are specific requirements to ensure that AI systems can be audited and that their operations are explainable to human operators.

4. Data Quality and Governance

- High-risk AI systems must be trained on datasets that meet high standards of quality, including accuracy, relevance, and representativeness. This is to mitigate risks such as bias and discrimination.
- AI providers are required to implement data governance measures to ensure the quality and integrity of the datasets used, including documentation and traceability.

6. Conformity Assessment and CE Marking

- High-risk AI systems must undergo a conformity assessment before being placed on the market. This assessment verifies that the system meets all the requirements of the AI Act.
- Once the assessment is passed, the AI system can receive a CE marking, indicating that it complies with EU safety, health, and environmental protection standards.

AI related regulation: EU AI Act (obligations not yet applicable)

(Continued)

7. Post-Market Monitoring and Reporting

- Providers of high-risk AI systems are required to implement post-market monitoring processes to track the performance of AI systems after they have been deployed. This includes collecting data on the AI system's operation and reporting any serious incidents or malfunctions to the relevant authorities.
- Continuous evaluation and improvement of AI systems are encouraged to ensure they remain compliant over time.

10. Governance and Enforcement

- The Act establishes a European Artificial Intelligence Board (EAIB) to facilitate the implementation and enforcement of the AI regulations across member states.
- National supervisory authorities will be responsible for monitoring compliance at the country level and coordinating with the EAIB on cross-border issues.

8. AI Regulatory Sandbox

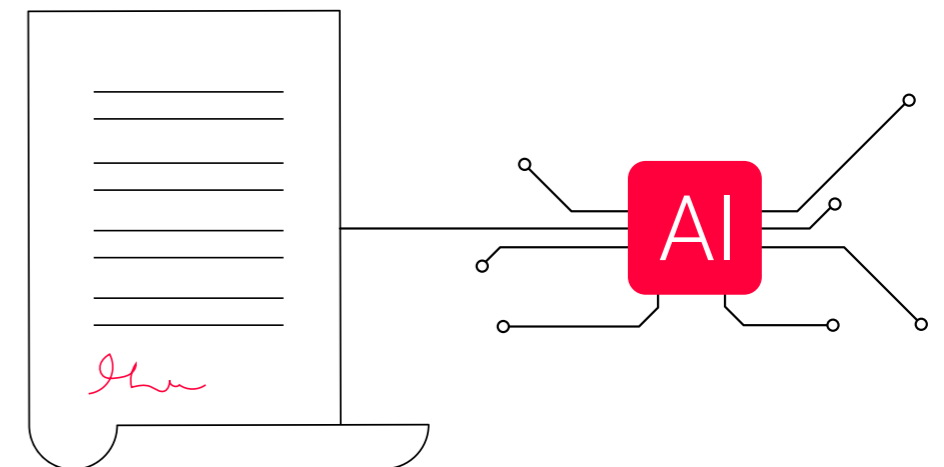
- The Act introduces the concept of “AI regulatory sandboxes,” which are controlled environments where companies can test innovative AI solutions under the supervision of regulators. This is designed to encourage innovation while ensuring compliance with legal and ethical standards.

11. Support for SMEs and Startups





- The Act includes provisions to support small and medium-sized enterprises (SMEs) and startups in complying with the regulations. This includes access to regulatory sandboxes and reduced fees for conformity assessments.

9. Penalties for Non-Compliance







- The Act proposes significant fines for non-compliance, with penalties of up to €30 million or 6% of the company's global annual turnover, whichever is higher, for the most severe breaches.
- Lesser violations may result in fines of up to €20 million or 4% of global turnover.







AI related regulation: Latin America

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Argentina</p>		<p>Personal Data Protection Law (Law No. 25,326)</p> <ul style="list-style-type: none"> • Governs the collection, processing, and storage of personal data in Argentina. <p>Copyright Law (Law No. 11,723)</p> <ul style="list-style-type: none"> • Protects the intellectual property rights of creators. <p>Trademark and Patent Laws</p> <ul style="list-style-type: none"> • Relevant if generative AI is used in ways that involve creating or altering trademarks or patented content. <p>Consumer Defense Law (Law No. 24,240)</p> <ul style="list-style-type: none"> • Protects consumers from misleading and deceptive practices.
 <p>Brazil</p>		<p>No. 5051 (2019)</p> <ul style="list-style-type: none"> • Prioritize human well-being and rights in the use of AI • Human oversight and supervision mechanisms should be informed by type, severity, and implications of decisions made by AI, where supervisors will be held liable for any harm resulting from AI systems. <p>No. 21/2020 (2020)</p> <ul style="list-style-type: none"> • Emphasizes ethical AI development, including respect for human rights, non-discrimination, privacy protection, transparency, and responsible innovation practices, aligning with international standards. <p>No. 872 (2021)</p> <ul style="list-style-type: none"> • Mandates AI to respect autonomy, preserve social and cultural diversity, enable democratic scrutiny, include security measures for human intervention, ensure traceable and unbiased decisions, and follow governance standards for risk management. • To promote inclusive growth and sustainable development, the bill requires the development of digital education, worker training in AI, gradual AI adoption, incentives for AI investment, cooperation between public and private sectors, and training opportunities for AI professionals.



AI related regulation: Latin America

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Chile</p>		<p>Bill 15869-19 (under deliberation at time of publishing)</p> <ul style="list-style-type: none"> • Regulates AI systems, robotics and related technologies. • Requires developers, suppliers, and users of AI systems to seek authorization prior to beginning development, marketing, distribution and use of systems in Chilean territory. • Classifies AI systems into “unacceptable risk” and “high risk”. • For high-risk systems, Commission will request applicant to comply with certain requirements prior to authorisation.
 <p>Columbia</p>		<p>059/23 on Public Policy Guidelines for AI</p> <ul style="list-style-type: none"> • Establishes public policy guidelines for the development, use, and implementation of AI. • Sets out principles for AI including human authority, common good, cooperation, safe design, prevalence of human intelligence, and preventive research.
 <p>Costa Rica</p>		<p>Law on the Protection of Individuals Regarding the Processing of Their Personal Data (Law No. 8968)</p> <ul style="list-style-type: none"> • Any generative AI system that processes personal data must comply with this law, which includes requirements for data consent, data security, and the rights of individuals regarding their data. <p>Copyright Law (Law No. 6683)</p> <ul style="list-style-type: none"> • Protects the rights of authors and creators over their intellectual property. <p>Consumer Protection Law (Law No. 7472)</p> <ul style="list-style-type: none"> • Aims to protect consumers from unfair practices and ensure that they are not misled by businesses.





AI related regulation: Latin America

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Dominican Republic</p>		<p>Law on the Protection of Personal Data (Law No. 172-13)</p> <ul style="list-style-type: none"> • Governs the collection, processing, and storage of personal data. <p>Copyright Law (Law No. 65-00)</p> <ul style="list-style-type: none"> • Protects the rights of authors and creators over their intellectual property. <p>Consumer Protection Law (Law No. 358-05)</p> <ul style="list-style-type: none"> • Protects consumers from unfair, misleading, or deceptive business practices. <p>General Telecommunications Law (Law No. 153-98)</p> <ul style="list-style-type: none"> • While not specific to AI, this law governs telecommunications and includes provisions that indirectly affect AI systems, especially those deployed in digital and online environments.
 <p>Mexico</p>		<p>Federal Law on the Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LFPDPPP)</p> <ul style="list-style-type: none"> • Governs the processing of personal data by private entities. <p>Federal Copyright Law (Ley Federal del Derecho de Autor)</p> <ul style="list-style-type: none"> • Protects intellectual property rights, including copyrights, and is crucial for generative AI, especially when it comes to the use of copyrighted materials in AI training datasets and the ownership of AI-generated content. <p>Industrial Property Law (Ley de la Propiedad Industrial)</p> <ul style="list-style-type: none"> • Deals with trademarks, patents, and other forms of industrial property. <p>Federal Consumer Protection Law (Ley Federal de Protección al Consumidor)</p> <ul style="list-style-type: none"> • Protects consumers from misleading, deceptive, or abusive practices by businesses.



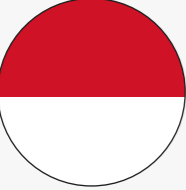

AI related regulation: Latin America

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Peru</p>		<p>Law on the Protection of Personal Data (Law No. 29733)</p> <ul style="list-style-type: none"> • Governs the processing of personal data in Peru. <p>Regulation of the Law on the Protection of Personal Data (Supreme Decree No. 003-2013-JUS)</p> <ul style="list-style-type: none"> • Provides further guidance on the implementation of the Personal Data Protection Law and details specific obligations for data controllers and processors, which would include those deploying AI systems. <p>Copyright Law (Legislative Decree No. 822)</p> <ul style="list-style-type: none"> • Protects the rights of creators and authors over their intellectual property. <p>Industrial Property Law (Legislative Decree No. 1075)</p> <ul style="list-style-type: none"> • Governs trademarks, patents, and other forms of industrial property. <p>Consumer Protection and Defense Code (Law No. 29571)</p> <ul style="list-style-type: none"> • Designed to protect consumers from unfair, misleading, or abusive practices by businesses.





AI related regulation: Asia Pacific

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Australia</p>		<p>Privacy Act 1988</p> <ul style="list-style-type: none"> Regulates how personal information is collected, used, stored, and disclosed; applies to businesses and organisations with an annual turnover exceeding AUD 3 million. <p>Australian Consumer Law (ACL)</p> <ul style="list-style-type: none"> Provides protections for consumers against unfair practices, misleading or deceptive conduct, and ensures product safety. <p>Copyright Act 1968</p> <ul style="list-style-type: none"> The law currently requires that for a work to be protected by copyright, it must have a human author. <p>AI Ethics Framework</p> <ul style="list-style-type: none"> A non-binding framework provides principles for the ethical use of AI, such as fairness, transparency, accountability, and respect for privacy.
 <p>China</p>		<p>Regulation on the Management of Deep Synthesis Technology (2023)</p> <ul style="list-style-type: none"> Addresses concerns about the misuse of technologies such as deepfakes, AI-generated text, images and audio, for creating misleading or harmful content. <p>Cyberspace Administration of China (CAC) Regulations</p> <ul style="list-style-type: none"> Addresses Content Control (e.g., AI-generated content does not contravene Chinese laws, especially regarding political sensitivity, social stability, and public morality) and Data Privacy. <p>Personal Information Protection Law (PIPL) (2021)</p> <ul style="list-style-type: none"> Similar to the EU's GDPR, it governs the collection, use, processing, and transfer of personal data. <p>Cybersecurity Law (2017)</p> <ul style="list-style-type: none"> Establishes general cybersecurity requirements for companies operating in China, including data localisation (storage) and cybersecurity review requirements.



AI related regulation: Asia Pacific

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Indonesia</p>		<p>Personal Data Protection Law (PDPL) (2022)</p> <ul style="list-style-type: none"> • Similar to the EU's GDPR, governs the collection, processing, storage, and transfer of personal data. <p>Electronic Information and Transactions Law (EIT Law) Law No. 11 of 2008 (amended by Law No. 19 of 2016)</p> <ul style="list-style-type: none"> • Regulates electronic information and transactions, including the use and dissemination of electronic content (content regulation and associated criminal liability). <p>Broadcast Law No. 32 (2002)</p> <ul style="list-style-type: none"> • AI-generated content that is broadcasted must comply with national broadcasting standards, including restrictions on content that could be politically sensitive, defamatory, or against public decency. <p>Various Kominfo Regulations</p> <ul style="list-style-type: none"> • Regulations that impact online content, data protection, and the use of electronic systems, including platform responsibility and data localisation.
 <p>Malaysia</p>		<p>Personal Data Protection Act 2010 (PDPA)</p> <ul style="list-style-type: none"> • Malaysia's primary data protection law, governing the collection, use, processing, and disclosure of personal data in commercial transactions <p>Communications and Multimedia Act 1998 (CMA)</p> <ul style="list-style-type: none"> • AI-generated content distributed online or through multimedia platforms must comply with the CMA's provisions, including content regulation and platform liability. <p>Consumer Protection Act 1999</p> <ul style="list-style-type: none"> • Covers issues such as product safety, misleading advertising, and unfair trade practices. <p>Copyright Act 1987</p> <ul style="list-style-type: none"> • Governs the protection of intellectual property rights in Malaysia, including works of art, literature, music, and software.

AI related regulation: Asia Pacific

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>Philippines</p>		<p>Data Privacy Act of 2012 (DPA)</p> <ul style="list-style-type: none"> • The Philippines' primary data protection law, governing the collection, processing, storage, and transfer of personal data by both public and private entities. <p>Consumer Act of the Philippines</p> <ul style="list-style-type: none"> • Provides protection for consumers against deceptive, unfair, and unsafe business practices. <p>Intellectual Property Code of the Philippines</p> <ul style="list-style-type: none"> • Governs the protection of intellectual property rights, including copyrights, patents, and trademarks. <p>E-Commerce Act of 2000</p> <ul style="list-style-type: none"> • Regulates electronic transactions and online business practices, including guidelines for content authenticity.
 <p>Singapore</p>		<p>Personal Data Protection Act (PDPA)</p> <ul style="list-style-type: none"> • Singapore's primary data protection law plays a significant role in regulating how AI systems, including generative AI, handle personal data. <p>Model AI Governance Framework</p> <ul style="list-style-type: none"> • Guides organizations in the responsible development and deployment of AI systems. <p>Sector-Specific Regulations</p> <ul style="list-style-type: none"> • Financial Services and Healthcare regulations ensure that AI systems are used in a way that is fair, ethical, accountable and transparent. <p>National AI Strategy</p> <ul style="list-style-type: none"> • Outlines the government's approach to AI development and deployment across various sector.

AI related regulation: Asia Pacific

Country	Specific legislation regulating use, development or deployment of AI	Existing legislation that might affect the use of AI Selective and non-comprehensive
 <p>South Korea</p>		<p>Personal Information Protection Act (PIPA)</p> <ul style="list-style-type: none"> • A comprehensive data protection law, regulating the collection, use, processing, and transfer of personal data. <p>Network Act (Act on Promotion of Information and Communications Network Utilization and Information Protection)</p> <ul style="list-style-type: none"> • Regulates information and communications networks in South Korea, focusing on the protection of personal information and the prevention of information leakage. <p>Artificial Intelligence Framework Act (to be implemented in 2024)</p> <ul style="list-style-type: none"> • Designed to promote the development and ethical use of AI technologies, including generative AI; includes ensuring that users are aware of when they are interacting with AI-generated content. <p>Ethical Guidelines for AI</p> <ul style="list-style-type: none"> • Not legally binding but set out ethical standards for the development and use of AI technologies, including generative AI.



World Federation of Advertisers
London, Brussels, Singapore, New York

wfanet.org

info@wfanet.org

+32 2 502 57 40

twitter @wfamarketers

youtube.com/wfamarketers

linkedin.com/company/wfa



R3 is an independent global marketing transformation consultancy. We work with marketers to enhance their return on marketing, media, and agency investment, and to improve efficiency and effectiveness. We enable our clients to achieve a competitive edge and a better return on investment from agencies, media and marketing spend.

www.rthree.com

**For further info please contact Sarah Tan, EVP,
Delivery, R3 at sarah@rthree.com**



Competition compliance policy

The purpose of the WFA is to represent the interests of advertisers and to act as a forum for legitimate contacts between members of the advertising industry. It is obviously the policy of the WFA that it will not be used by any company to further any anti-competitive or collusive conduct, or to engage in other activities that could violate any antitrust or competition law, regulation, rule or directives of any country or otherwise impair full and fair competition. The WFA carries out regular checks to make sure that this policy is being strictly adhered to.

As a condition of membership, members of the WFA acknowledge that their membership of the WFA is subject to the competition law rules and they agree to comply fully with those laws. Members agree that they will not use the WFA, directly or indirectly, (a) to reach or attempt to reach agreements or understandings with one or more of their competitors, (b) to obtain or attempt to obtain, or exchange or attempt to exchange, confidential or proprietary information regarding any other company other than in the context of a bona fide business or (c) to further any anti-competitive or collusive conduct, or to engage in other activities that could violate any antitrust or competition law, regulation, rule or directives of any country or otherwise.

Please note that the recommendations included in this document are merely meant as suggestions or proposals. They are not binding in any way whatsoever and members are free to depart from them.