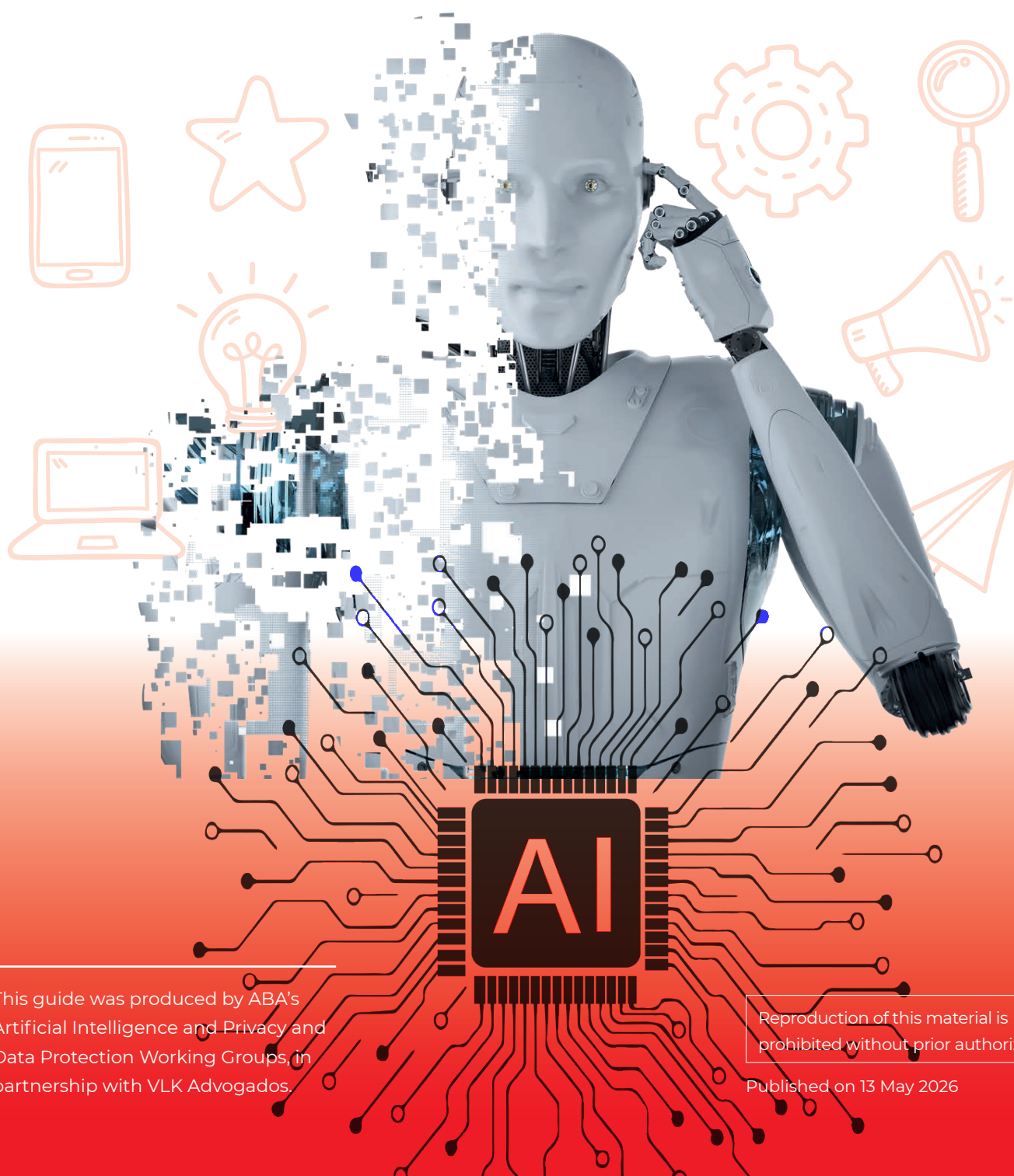


Best Practices Guide for Data and AI in Marketing



This guide was produced by ABA's Artificial Intelligence and Privacy and Data Protection Working Groups, in partnership with VLK Advogados.

Reproduction of this material is prohibited without prior authorization.

Published on 13 May 2026

Introduction

Communication and marketing are undergoing a profound transformation driven by the convergence of the online and offline worlds, where the constant interconnection between people, platforms, and devices generates information and digital traces that feed artificial intelligence tools, revolutionizing communication between brands and consumers and democratizing access to resources that enable the creation of highly customized and persuasive content.

In this context, the intensive use of data has become the true fuel for the application of AI systems (especially generative AI), which are already part of content creation, planning, and media buying routines, directly impacting marketing campaigns that are increasingly personalized and relevant, strengthening relationships and loyalty between brands and consumers.

Currently, it is virtually impossible to separate personal data processing from marketing activities. AI algorithms depend on large volumes of information to train models, generate insights, and accurately anticipate behavior. Data enables audience understanding, measurement, and personalization; AI enhances the ability to create, test, and optimize at scale. Together, these technologies are reshaping the advertising chain, from briefing and content production to media buying, customer service, and research for insight generation.

This synergy brings clear benefits to the market, such as greater time and cost efficiency through task automation, enhanced analytical capability in handling large volumes of information, and the ability to deliver more relevant and personalized experiences at scale, while maintaining consistency and execution speed.

At the same time, this technological advancement increases responsibilities and areas of attention that cannot be treated merely as “technical details.” The combined use of data and AI increases exposure to legal, reputational, and ethical risks, with a direct impact on consumer trust and the sustainability of the advertising ecosystem. Responsible adoption requires governance with controls proportional to the level of technological risk involved (definition of roles and responsibilities, transparency, explainability, human review and supervision, traceability, data management, documentation, and incident response), which may increase regulatory

and reputational risks — ranging from misleading advertising and algorithmic discrimination to violations of privacy, copyright, and personality rights. In the Brazilian legal context in particular, compliance in the use of these technologies requires an integrated interpretation of applicable rules and best practices, such as the General Data Protection Law (LGPD), the Consumer Protection Code (CDC), Copyright Law, advertising self-regulation, the EU AI Act, NIST frameworks, and ISO/IEC standards.

It is within this context that ABA, in partnership with VLK Advogados, presents the ABA Guide to Best Practices for the Use of Data and AI in Marketing. The objective is to help the market anticipate these challenges by organizing and establishing concrete, applicable, and verifiable standards that guide advertisers, agencies, platforms, and service providers in the lawful, ethical, and safe use of personal data and AI, in full alignment with advertising self-regulation and current legislation.

“By leading this movement, the industry enhances legal certainty, consolidates the protection of rights, and strengthens consumer trust, acting strategically in the construction of a balanced regulatory environment, reducing uncertainties, anticipating risks, and avoiding interpretations that could stifle innovation or restrict creative freedom,” emphasizes Nelcina Tropardi, President of ABA and VP Legal, Corporate Affairs, Compliance, Inclusion and Diversity, ESG, Risk Management, and Corporate Communications at Carrefour.

“In an era marked by the speed of technological innovation in pursuit of efficiency and personalization through the intensive and increasingly sophisticated use of personal data and AI, it becomes important that the development of regulatory frameworks includes the active participation of the market itself. Self-regulation initiatives and the consolidation of best practices help reduce asymmetries of knowledge between the State and society, incorporating practical business experience. By leading this agenda, ABA contributes to strengthening legal certainty, balancing the protection of fundamental rights with economic and technological development. Law acts as an enabler of innovation, including in modern forms of regulating communication and marketing, boosting the creative economy and strengthening consumer trust,” emphasize Rony Vainzof and Gisele Karasawa, partners at VLK Advogados.

Introduction

“The guide was structured to transform regulatory and technological concerns into practical guidance applicable to the day-to-day operations of the sector. By bringing together essential concepts, legal foundations, principles, and operational best practices from the two pillars that currently shape contemporary marketing—data protection and the use of AI—we aim to support strategic decision-making, guide contracting processes, improve internal workflows, strengthen governance structures, and raise standards of transparency and accountability in communication with the public,” comments Paula Ercole Bauléo, Leader of ABA’s AI Working Group and Senior Legal Manager at General Mills.

“This document constitutes a reference framework for the adoption of policies, processes, and governance aligned with applicable legislation, advertising self-regulation, and national and international best practices, also serving as a technical parameter for regulators and the Judiciary in interpreting conduct, risks, and standards of diligence within the sector,” concludes Rodrigo Borges, Leader of ABA’s Data Protection and Privacy Working Group and Director of Privacy - Latin America at Kenvue.

“The Guide fills a real gap. The market is already using AI in content production, targeting, and media buying, but most organizations still govern this use in a fragmented way, without connecting LGPD requirements, self-regulation rules, and contractual obligations into a workable architecture. What this document does is exactly that: translate a dispersed set of norms and best practices into guidance applicable to the full operational cycle. For legal teams working close to the product, this is the kind of input that enables governance to be built before the incident, not after it,” says Lucas Gobbo, Co-Leader of ABA’s Data Protection and Privacy Working Group and Global Legal Manager & Product Counsel at BEES - AB InBev.

Note on international references:

References to foreign authorities, standards, and materials throughout this Guide are used for comparative, technical, and informational purposes, as sources of best practices and regulatory trends. Such references are not binding in Brazil, except where there is specific legal or regulatory applicability to a given operation, agent, or territory.

This Guide is based on what ABA has been building with pioneering spirit and consistency since the creation of its Privacy and Data Protection and Artificial Intelligence Working Groups. These groups have been making continuous efforts to promote qualified debate on technology, innovation, and responsibility in marketing, developing shared understandings and disseminating technical and qualified knowledge through initiatives that include guidance materials, advocacy actions, and agendas aimed at fostering institutional dialogue with relevant stakeholders. This collective effort was also recognized with the Marketing Best 2025 Award, Technology category, for the case “ABA Best Practices for the Use of Artificial Intelligence in Marketing,” which reflected a consistent set of deliverables over recent years, including publications and initiatives also developed in partnership with VLK.

By consolidating this knowledge into a best practices guide, the organization seeks to contribute to a responsible innovation environment in which the use of data and artificial intelligence is guided by fundamental principles of ethical advertising, such as respect for consumers, integrity of communication, data protection, and responsibility in the adoption of new technologies. At the same time, the Guide is intended to serve as a national and international benchmark, reinforcing Brazil’s role in the global debate and valuing the concrete experience of advertisers.

More than a static document, this Guide is intended to be a living reference for the market—open to evolution, improvement, and updates—and an invitation for the entire advertising ecosystem to advance collaboratively in building increasingly innovative, transparent, and responsible marketing practices. We believe it is possible—and necessary—to advance with technology without renouncing the principles that guide ethical advertising, such as respect for consumers, integrity of communication, data protection, and responsibility in the adoption of AI.



Sandra Martinelli

CEO of ABA – Brazilian Association of Advertisers
and Member of the WFA Executive Committee

Table of Contents

I - Personal Data Protection in Marketing	08
1. Why Data Protection is a strategic issue for marketing	09
2. Advertising chain and data processing agents	10
3. Principles of the LGPD applied to marketing in practice	14
3.1. Purpose	14
3.2. Adequacy & Necessity	14
3.3. Transparency	15
3.4. Security & Prevention	17
4. Legal bases in digital marketing	18
4.1 Brazil vs Europe	18
4.2 Consent and legitimate interest: when to use each one	19
4.3 Cookies and first-party	22
4.4 Sensitive data in marketing	24
4.5 Consent or Pay	25
5. Targeted advertising and profiling	27
6. Programmatic advertising and adtech ecosystem	30
7. International data transfers in marketing	31
8. Children and adolescents in digital marketing	33
 II - Artificial Intelligence in Marketing	 37
1. Traditional AI vs generative AI in marketing	38
2. Where AI fits into the advertising value chain	38
2.1 Chain actors: who does what and where AI typically enters	39
2.2. AI as a tool, creative partner and legal risk	40
2.3 Responsibility across the chain	41
3. Real-world use cases of AI in marketing	43
3.1 Content creation (text, image, video, audio and variations)	44
3.2. Media and optimization (buying, targeting, bidding and real-time decision-making)	46
3.3. Measurement and attribution	47
3.4 Customer service and research (chatbots, agents and market research)	48

4. Principles that should govern Responsible and Ethical AI in Marketing	49
4.1. Legitimate purpose and business alignment	49
4.2. Transparency and risk – proportionate explainability	50
4.3. Human centrality and supervision	51
4.4. Non-discrimination, fairness and bias mitigation	52
4.5. Security, integrity and reliability	53
4.6. Responsibility and accountability	54
4.7. Legal and regulatory compliance	54
4.8. Proportionality between risk, control and impact	56
5. Key risks and practical safeguards	57
5.1. Deceptive or abusive advertising, AI washing and claims about AI	58
5.2. Synthetic content and integrity	59
5.3 Synthetic personas and synthetic data	60
5.4 Bias, discrimination and stereotypes	62
5.5 Intellectual property and personality rights	63
5.6. Personal data in AI training	65
5.7. Information security in AI	67
5.8. Children and vulnerable groups: enhanced safeguards (content, targeting, persuasion)	71
5.9. Sustainability and social impacts (energy, supply chain, reputation)	72
6. AI governance applied to advertising (How to implement it)	74
6.1 Transparency with the public: when and how to disclose the use of AI	74
6.2 Assessment for the hiring of agencies	76
6.3 Internal policies and training	77
6.4 Selection and approval of tools	77
6.5. Governance gate before go-live	78
6.6 Operational workflow with AI (End-to-end)	79
6.7 Traceability and documentation	79
6.8 Incident management and rapid response	80
Conclusion	82

▶▶ CHAPTER I

Personal Data Protection in Marketing



1. Why Data Protection is a strategic issue for marketing

Personal data has taken on a central role in marketing, as it has moved beyond being merely an operational input to becoming a true business asset, capable of guiding decision-making, personalizing experiences, and maximizing results.

In parallel, the consolidation of global regulatory frameworks such as the GDPR, the LGPD, and more than 130 similar laws has redefined structural parameters for data processing in advertising activities. Far from making data-driven advertising unfeasible, these rules have established objective criteria for its responsible use, setting out legal bases, governance structures, and accountability mechanisms.

This shift has overcome the inefficient model of near-total reliance on consent, opening space for more sophisticated, sustainable, and legally secure approaches. The result is an environment in which data can drive innovation and performance, provided it is integrated into a consistent strategy of compliance, ethics, and risk management.

In this context, consumer trust emerges as a decisive competitive advantage. Brands that demonstrate transparency, responsibility, and respect for privacy tend to build longer-lasting and more valuable relationships with their audiences, while opaque or abusive practices generate not only legal sanctions but also significant reputational damage.

Ethical and transparent use of data therefore strengthens brand image and prevents communications from being perceived as intrusive or manipulative. Effective advertising depends on a relationship of trust; audiences need to believe that the information they receive is reliable and that their privacy is respected.

A 2024 study conducted by PwC showed that 90% of Brazilian consumers believe that the protection of their data is one of the most important factors for companies to earn their trust¹.

Thus, the LGPD should not be understood or interpreted as an obstacle to marketing and advertising activities, but rather as a structural element of how marketing and advertising operate in practice. Integrating data protection into communication and relationship strategies is, today, an essential condition for the sustainability, credibility, and effectiveness of market actions.

¹<https://www.pwc.com.br/pt/sala-de-imprensa/release/90-dos-consumidores-brasileiros-afirma-que-a-protecao-dos-seus-dados-possuio-um-dos-fatores-mais-importantes.html>

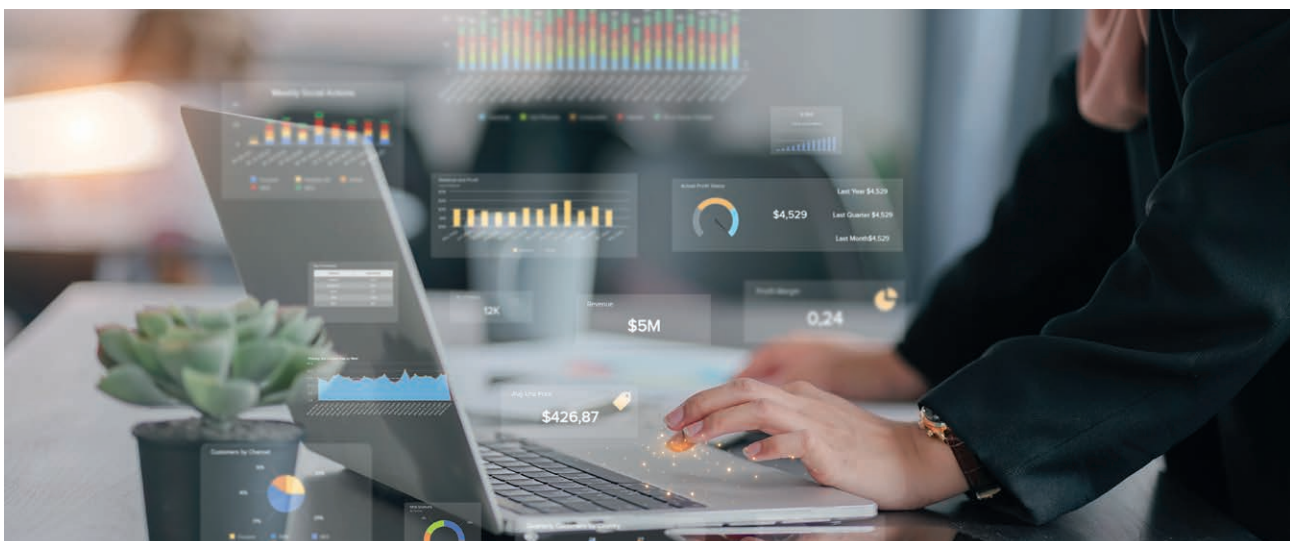
2. Advertising Chain and Data Processing Agents

Data processing agents are the entities to which legislation assigns duties and responsibilities in the context of data protection, defined based on their decision-making power over the purposes and means of processing, or their role in carrying out such activities.

In the context of the advertising chain, it is essential to accurately identify who these agents are, which decisions they effectively control, and which operations they perform, as this delineation structures the allocation of responsibilities and the distribution of risk.

Data processing agents can be divided into two categories²:

Controller	The entity responsible for making essential decisions regarding the processing of personal data, in particular the purposes, the nature of the personal data, the specific data required, and the duration of the processing. Its defining characteristic is decision-making power.	As a general rule, the Controller is responsible for ensuring the lawfulness of the processing, while the Processor must comply with the Controller's lawful instructions and ensure that the processing entrusted to it is performed securely and can address any data subject rights requests.
Processor	Agent that performs data processing activities on behalf of the Controller, following its instructions, while being able to make non-essential decisions. For example, decisions regarding the software or hardware to be used.	



² <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-para-definicoes-dos-agentes-de-tratamento-de-dados-pessoais-e-do-encarregado> and https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

These categories of data processing agents may interact in four different ways:

Independent Controllers	The Parties carry out their own processing activities, independently determining the essential elements of such processing.
Joint Controllers	The essential elements of the processing are defined jointly, either through a common decision (the parties jointly participate in decision-making) or through converging decisions (the parties make separate but complementary decisions, both of which are necessary for the essential elements of the processing activity).
Controller–Processor	One party (Processor) performs a processing activity whose essential elements are defined by another party (Controller).
Processor–Subprocessor	A Processor subcontracts the performance of the processing activity to a third party (Subprocessor).

ATTENTION!

A processor may be deemed equivalent to a controller when it fails to comply with the controller's lawful instructions and independently and improperly determines the purposes and means of processing³.

Actors in the advertising chain and their typical roles.⁴

ADVERTISER

Who are they?	Role (as a rule)
Entities that promote their products, services, or brands through marketing strategies and advertising campaigns.	They will be considered controllers of activities related to the collection, use, and potential sharing of personal data whenever they define the purposes and means used to target advertisements to audiences, whether on websites or specific platforms. They may also be characterized as controllers in situations where, even without directly carrying out the processing of personal data, they participate in determining the type of information they wish to receive and the purpose for which it will be used, such as when contracting a market research company by defining demographic, behavioral, or interest-based characteristics of the intended audience ⁵ .

³ According to the LGPD (Art. 42, §1, I), the Processor shall be jointly and severally liable for damages caused by the processing when it fails to comply with data protection obligations or when it has not followed the Controller's lawful instructions, in which case the Processor is deemed equivalent to the Controller. See also: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#4>

⁴ https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf;

<https://publya.com/blog/glossario-da-midia-programatica/>; <https://www.gdpr-impact.com/>;

https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_socialmedia_users_en.pdf

⁵ https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pt.pdf, page 20

PUBLISHERS

Who are they?	Role (as a rule)
Owners of websites, apps, and other digital environments that provide advertising space, monetizing it through SSPs or ad networks.	They will be considered controllers with respect to the collection and sharing of their users' data, and do not act as controllers in relation to the processing activities carried out with such data by other actors in the chain once it has been shared.

AD NETWORKS

Who are they?	Role (as a rule)
Intermediaries between advertisers and publishers, aggregating advertising inventory and facilitating its commercialization.	They will be considered controllers in view of their role in collecting personal data from multiple publishers, building behavioral profiles, and selecting which advertisement to display to each user.

DEMAND-SIDE PLATFORMS (DSPS)

Who are they?	Role (as a rule)
They are platforms used by advertisers to purchase advertising inventory.	Whenever they do not make decisions regarding data and act solely on behalf of advertisers to execute advertising in a cost-efficient manner, they will be considered processors.

SUPPLY-SIDE PLATFORMS (SSPs)

Who are they?	Role (as a rule)
They are platforms used by publishers to sell advertising inventory.	Whenever they do not make decisions regarding data and merely aggregate publishers' advertising inventory ⁶ , they will be considered processors.

DATA MANAGEMENT PLATFORMS (DMPs)

Who are they?	Role (as a rule)
Platforms used to collect, organize, and segment audience data.	Whenever they merely provide technological infrastructure for managing data used in advertising and do not make decisions regarding the essential elements of the data, they will be considered processors.

⁶ <https://www.jipitec.eu/jipitec/article/download/410/411/2152>



ATTENTION!

DSPs, SSPs and DMPs: although they act as data processors when performing their core functions, they may be classified as independent controllers or joint controllers depending on their business model and level of decision-making regarding data collection, matching, enrichment, and any subsequent use of data for their own purposes.

For risk mitigation purposes, the responsibilities assigned to each of the involved parties must be clearly and unequivocally defined through formal contractual arrangements, which, based on NBR ISO/IEC 27701, should establish:

For contracts between controllers	For contracts with processors
• Purposes of processing and data sharing • Definition of the categories of personal data subject to processing • General description of the processing activities (e.g., how the data must be used) • Responsibilities for implementing technical and administrative security measures • Responsibilities in the event of security incidents • Responsibilities and retention and deletion periods for the data • Responsibilities and points of contact for handling data subject requests • Responsibilities regarding transparency of the processing activities towards data subjects	• Purpose of Processing and prohibition of processing for any other purpose • Categories of data processed and categories of data subjects • Definition of security obligations related to the processing of personal data • To notify security incidents to the Controller without undue delay • Cooperation in incident response, with clearly defined timelines • Assistance to the Controller in responding to data subject and ANPD requests • Subcontracting of processing activities (possibility, approval criteria, and notification requirements) • Log recording and retention • Data retention and deletion • Return and deletion of data upon termination of the contract

3. Principles of the LGPD Applied to Marketing in Practice

Although there is no hierarchical order among the principles of the LGPD, four of them require special attention in the context of marketing activities: purpose limitation, adequacy, necessity, and transparency.

3.1 Purpose

Processing activities must have a specific, lawful, explicit purpose that is communicated to the data subject.

In the context of marketing, this means that before processing any personal data for advertising campaigns, it is necessary to ask: what is the campaign intended to achieve? Who is the target audience?

These and other information must be clearly defined from the campaign briefing stage and must guide the entire data lifecycle (from collection to deletion), as well as all stages of the advertising campaign (e.g., from campaign design to execution and post-campaign activities).

3.2 Adequacy & Necessity

The principles of adequacy and necessity, considered together, require that personal data processing constitutes an effective means to achieve the intended purpose and is limited to the minimum necessary for that purpose.

This implies that:

- the personal data processed and the channels used must be suitable for achieving the legitimately intended objective
- their use must fall within the reasonable expectations of the data subject
- both the data and the channels used must be reasonably necessary to achieve the intended purpose

BUT WHAT IS “NECESSARY”?

-  Necessary does not mean “absolutely essential”
-  Necessary does not mean useful or customary
-  Necessary means being a reasonable and proportionate means of achieving the intended purpose⁷

⁷ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/>

Practical recommendations for compliance with the principles of Adequacy & Necessity:	
When selecting a channel	✓ Assess whether the data subject can reasonably expect to receive that advertising through the intended channel ✓ Verify whether the channel is suitable for your target audience
When selecting data	✓ Carefully assess how the data to be used is relevant and useful for the campaign ✓ Consider whether the data subject can reasonably expect their data to be used for the campaign in question ✓ Assess whether the selected data could be regarded as excessively intrusive from a privacy perspective

ATTENTION!

Temporal limitation of processing: personal data cannot be retained indefinitely, and its retention after the purpose for which it was collected has ended must be justified.

- Advertising is a continuous process of behavioral analysis. If the purpose of data collection is defined as “customer relationship management” or “promotion of products of brand X,” retention may no longer be tied to a specific advertising piece and may instead extend to the long-term marketing strategy
- It is important to periodically review retention practices and implement data minimization plans, discarding what has become obsolete or excessive, and documenting in Records of Processing Activities (RoPA) how informed reuse benefits data subjects (e.g., more relevant offers), as well as how the retention period was calculated to ensure it is not excessive

3.3 Transparency

The principle of transparency requires that “clear, precise, and easily accessible” information about personal data processing be provided. It is also a foundation of trust, as in data-driven marketing, transparency mitigates reputational risks, avoids perceptions of manipulation, and can improve campaign performance (fewer rejections, fewer opt-outs).

Properly implemented transparency does not reduce performance. On the contrary, it improves audience quality and strengthens long-term relationships.

What must be informed?

The minimum content of the information to be provided is defined in art. 9 of the LGPD:

- ✓ Specific purpose of the processing
- ✓ Form and duration of the processing, observing trade and industrial secrets
- ✓ Identification of the controller
- ✓ Contact information of the controller
- ✓ Information on the sharing of data by the controller and its purpose
- ✓ Responsibilities of the agents involved in the processing
- ✓ Rights of the data subject

Note: if the processing involves artificial intelligence, this is important information to be included when describing the “form” of processing.

ATTENTION!

In cases where the activity involves international data transfer, additional information must be provided:

- ✓ The form, duration, and specific purpose of the international transfer
- ✓ The destination country of the transferred data
- ✓ Identification and contact details of the controller
- ✓ Data sharing by the controller and its purpose
- ✓ The responsibilities of the processing agents involved and the security measures adopted
- ✓ The rights of the data subject and the means for exercising them, including an easily accessible channel and the right to file a complaint against the controller before the ANPD

It is also advisable for communication to explain in concrete terms the value generated for the user by the data; indicate whether it is used for personalization of offers, behavioral segmentation, training or improvement of AI models, and enrichment with third-party data.

As important as ‘what’ to inform is ‘how’ to inform it.

This means translating legal obligations into an efficient communication architecture. Considering the dynamic and highly visual nature of the advertising ecosystem, it is not recommended that the information provided to the data subject compromise the user experience, especially in light of the requirement that such information be easily accessible.

In this context, the use of overly technical or legalistic language (“legalese”) should be avoided, with preference given to simple, direct, and objective language, preferably supported by visual resources that enhance clarity and understanding of the content.

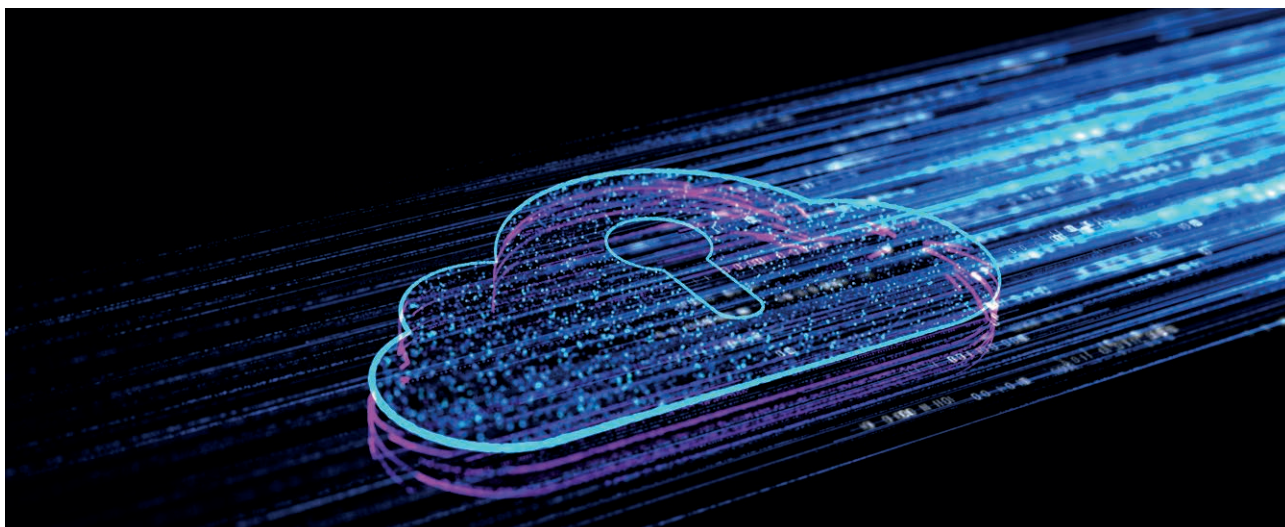
In other words, the same level of attention given to user experience in the design of a landing page, for example, should also be applied to the presentation of privacy and personal data protection information, ensuring consistency and end-to-end consumer engagement in brand communication.

Depending on the case, a “Layered Notices” approach may be adopted to balance the duty to inform with the need to maintain a smooth user journey:

- **Layer 1 (Interactive and Visual):** At first contact (e.g: banner or registration screen), only critical information should be provided in a concise and visual form, using icons and straightforward language. Focus on the specific purpose and the benefit to the user (e.g., “We use personal data to suggest offers that best match your preferences”)
- **Layer 2 (Detailed):** Through an easily accessible link, provide the full technical content required under Article 9 of the LGPD
- **Layer 3:** FAQs and practical examples

3.4 Security & Prevention

Advertising chain actors must adopt technical and administrative measures capable of protecting personal data against unauthorized access and accidental or unlawful destruction, loss, alteration, disclosure, or dissemination (Art. 6, VII, LGPD). Prevention (Art. 6, VIII) requires that risk mitigation measures be implemented before risks materialize, not only as a response to incidents.



4. Legal Bases in Digital Marketing

Legal bases are legal grounds that authorize the processing of personal data.

Legal Bases for the Processing of Personal Data	Legal Bases for the Processing of Sensitive Personal Data
• Consent • Compliance with a legal or regulatory obligation by the controller • Implementation of public policies • Performance of studies by a research body • Performance of a contract or preliminary contractual procedures • Regular exercise of rights • Protection of life or physical safety • Health protection • Legitimate interest • Credit protection	• Specific and highlighted consent • Compliance with a legal or regulatory obligation by the controller • Implementation of public policies • Conducting studies by a research body • regular exercise of rights • Protection of life or physical safety • Health protection • Ensuring fraud prevention and data subject security

There is no hierarchy among the legal bases provided for in the LGPD—meaning that the Controller has discretion to choose the legal basis that best fits the processing activity, provided that it is effectively applicable to the specific case.

In the context of marketing activities, two legal bases tend to be more commonly applicable: consent and legitimate interest. For this reason, this guide focuses specifically on the analysis of these two legal grounds.

4.1 Brazil vs. Europe

Although Brazilian legislation was inspired by the European model, the respective regulatory ecosystems are not identical. The European framework, for example, includes specific rules that more restrictively impact advertising activities, particularly the ePrivacy Directive and its transpositions into national laws, which impose consent as a requirement for various advertising activities⁸. The Digital Omnibus initiative even proposes amendments to these rules in an attempt to reduce the phenomenon of “consent fatigue”.

⁸ https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/#what_technologies_does_PECR_apply_to

In Brazil, legitimate interest may be legally applicable to certain marketing activities, provided that its appropriateness is assessed on a case-by-case basis and properly demonstrated through a balancing test, weighing the legitimacy of the interest, the necessity of the processing, the impacts on data subjects' rights, and their legitimate expectations. This assessment must be even more rigorous when involving children and adolescents, in compliance with the principle of the best interests of the child and the specific restrictions applicable to this audience, including those set forth in the Brazilian Digital Child and Adolescent Statute (ECA Digital), as discussed in item 8 of this Guide.

In this regard, the ICO states that, when not prohibited by specific regulation (which, again, does not exist in Brazil), targeted marketing activities may be considered a “legitimate interest,” provided that they satisfy the necessity and proportionality tests⁹.

4.2 Consent and Legitimate Interest: When to Use Each One

The application of this legal basis requires that the Controller's legitimate interests be proportionate to the impacts on the data subject's rights and freedoms.

A **documented Balancing Test** is the most appropriate way to assess and demonstrate the proportionality of legitimate interest and consists of the following stages:

- **Purpose Test:** to identify whether the processing is compatible with the legal framework, based on a concrete situation, and linked to a legitimate, specific, and explicitly defined purpose
- **Necessity Test:** to verify whether the processing of personal data is a reasonable and proportionate means of achieving the intended purpose, while processing the minimum amount of data possible
- **Proportionality Test:** to assess the risks and impacts of the processing on the rights and freedoms of data subjects and their proportionality in relation to the interests pursued

As the context and the processing activities themselves may change over time, it is recommended that the test be periodically reviewed.

Note: the ANPD provides a balancing test template in its guidance on legitimate interest¹⁰.

 **IMPORTANT!** In addition, when the processing activity is carried out on a large scale or may significantly affect the data subject's rights or relevant interests, it is advisable, in addition to the balancing test, to prepare a Data Protection Impact Assessment (DPIA).

⁹ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities.

¹⁰ https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf

PRACTICAL APPLICATION IN MARKETING: when is it more appropriate to use legitimate interest?

Although it is not possible to define, in the abstract, the situations in which legitimate interest is legally appropriate, there are factors that help determine whether processing may rely on this legal basis:

✓ No processing of sensitive personal data

Legitimate interest is only applicable to the processing of ordinary personal data

✓ Soft opt-in

As a rule, the existence of a prior relationship between the controller and the data subject positively impacts the legitimate expectation that their personal data may be processed for advertising purposes¹¹. It is important to emphasize that soft opt-in does not replace the need to ground the processing activity on a legal basis or to ensure transparency toward the data subject

✓ Easy opt-out

The right to object must be fully guaranteed, enabling the data subject to request the interruption of the processing in a simple and accessible manner¹²

✓ Transparency

The more clearly, directly, and unequivocally informed the data subject is, the greater the likelihood that the processing activity may legitimately rely on legitimate interest

✓ Respect for privacy

The lower the degree of intrusion regarding personal data and its origin within the data subject's sphere of privacy, the greater the likelihood that the processing activity may appropriately fall under the legal basis of legitimate interest

APPROPRIATE:	INAPPROPRIATE:
✓ Sending marketing emails to a database of customers or leads who provided their contact information ✓ Use by an e-commerce platform of information regarding the data subject's browsing and/or purchase history on its own platform to offer products likely to be of interest ✓ Customer profiling to identify potential churn cases (loss of customers and/or revenue) and enable preventive action ✓ Demographic segmentation of the lead database for targeted offers	✗ Building profiles based on sensitive personal data ✗ Invasive tracking of the data subject's activity across multiple websites, without adequate transparency, for the creation of behavioral profiles ✗ Persistent direct contact without a prior relationship with the data subject

¹¹ https://ferramentas.download.uol.com.br/uolhost/contratos/Codigo_de_Autorregulamentacao_para_pratica%20_de_email_Marketing.pdf

¹² <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/>



But what about consent?

- It may be used as an alternative to legitimate interest when there is a high level of intrusion, absence of a prior relationship, reduced data subject expectations, or the use of sensitive data. When properly implemented, it tends to strengthen the relationship of trust between the Advertiser and the data subject
- However, its adoption must be carried out carefully (preferably in situations where legitimate interest is not applicable), since it is subject to strict validity requirements. Improper implementation may compromise the lawfulness of the processing activity^{13,14}

★ **REMEMBER:** unlike consent, which transfers the initial decision to the data subject, legitimate interest requires greater internal accountability, as the controller bears the burden of demonstrating that the processing is proportionate and legitimate.

¹³ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>.

¹⁴ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

USE OF CONSENT AS A LEGAL BASIS IN THE MARKETING CONTEXT

Requirement: consent must be...	Applying it in practice
Freely given: the data subject must have a genuine choice not to consent (a merely formal authorization is not sufficient). Whenever possible, there should be a concrete option to refuse without causing detriment to the data subject	✓ Consent must not be required as a condition for obtaining a benefit or service that is not dependent on the processing activity ✓ Each purpose must be subject to separate consent
Informed: the data subject must receive sufficient information about the processing activity to make a conscious decision regarding it	✓ Prepare a consent form (see item 3 of this Guide for requirements) ✓ Present information in layers ✓ The first layer (opt-in) should contain a summary of the processing activity to be carried out, including the personal data elements most relevant to the data subject, accompanied by a link to the consent form
Unambiguous: the data subject must provide consent through a clear affirmative statement of intent (there is no consent by omission)	✓ Use checkboxes (always unchecked by default) or other similar mechanisms ✓ Only begin data collection after the data subject has affirmatively provided consent
Specific purpose: consent cannot be provided in abstract terms or for generic purposes	✓ Carefully define the specific purpose of the processing activity ✓ Present the purpose in a clear and objective manner ✓ Where multiple layers of information exist, the purpose must always be highlighted in the first layer
Highlighted: consent must be clearly distinguished from other terms (e.g., terms of use, contracts, etc.)	✓ Separate the consent form from other legal documents ✓ In the layer where consent is obtained, it must be separated from other consents

Consent fatigue: the indiscriminate use of consent may lead to request overload, automatic and poorly considered decisions by data subjects, reduced effective understanding, and loss of brand credibility. In other words, excessive and poorly structured consent mechanisms do not strengthen data protection. On the contrary, they weaken the user experience and may compromise legal validity.

4.3 Cookies and first-party

In its guidance document, the ANPD presumes that cookies used for advertising purposes generally do not fall under the legal basis of legitimate interest¹⁵.

¹⁵ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>

However, as already clarified, unlike in the EU, where the collection of consent for advertising cookies results from a specific requirement under the ePrivacy Directive, there is no equivalent obligation under the LGPD.

This presumption, therefore, cannot be treated as absolute, under penalty of violating the constitutional principle of legality, since the LGPD does not establish a hierarchy among legal bases.

FIRST-PARTY COOKIES: There are measures capable of supporting the classification of the processing activity under the legal basis of legitimate interest under Brazilian law (see the “Attention” box and the guidance on transparency, policies, and banners below), among which the use of first-party cookies stands out, that is: cookies created and used exclusively by the website accessed by the data subject and linked to its own domain¹⁶. Unlike third-party cookies, they do not generally imply the automatic sharing of data with external providers aimed at broad profiling of the data subject across different internet applications accessed by them.

 ATTENTION!

Although first-party cookies significantly reduce privacy risks when compared to third-party cookies, it is essential that reliance on legitimate interest always be subject to a concrete assessment, preferably formalized through a balancing test.

This is because there may be situations in which the collection of browsing information within the organization’s own internet application results in the disclosure of information intrusive to the data subject’s private sphere, including sensitive personal data.

By way of example, tracking a data subject’s activity on a dating website may reveal sexual preferences, which constitute sensitive personal data, making legitimate interest, consequently, an inadequate legal basis.

THIRD-PARTY COOKIES: As there is no hierarchy among legal bases for the use of cookies, companies may rely on either Legitimate Interest or Consent, depending on the nature of the campaign and the level of intrusiveness involved. Although the ANPD Cookie Guidance favors consent, it is important to note that legitimate interest may also be applicable, especially when personalization aims at marketing efficiency and consumer benefit (e.g., relevant offers), provided that it is accompanied by full transparency, respect for user expectations, low intrusiveness of the information collected and processed, and the guarantee of an easy opt-out mechanism. The decision should be supported by a documented Legitimate Interest Assessment (LIA), balancing business interests against consumer rights and ensuring that tracking is neither abusive nor unexpected.

¹⁶ https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf

TRANSPARENCY: Regardless of the legal basis adopted, it is essential to ensure transparency and, where applicable, the proper collection of consent and, in all cases, a clear and effective possibility for managing privacy preferences. In the context of cookie usage, these requirements are generally fulfilled through two main mechanisms: (a) the preparation of a Cookie Policy, either as a standalone document or integrated into the Privacy Notice; and (b) the implementation of a cookie banner with functional and accessible cookie management options.

COOKIE POLICY: The document follows the same requirements applicable to the Privacy Notice discussed above, with a focus on the processing activities carried out through cookies¹⁷. It is common market practice to specify which cookies are used, their respective purposes, and their retention periods.

COOKIE BANNER: This is a tool that assists organizations in accordance with the LGPD by providing data subjects with clear and automated information regarding the processing of their personal data and allowing them to manage their privacy preferences. Typically, these tools are structured in two layers.

- In the first layer, the cookie banner should provide the data subject with a clear summary of the purposes for which their data may be processed through cookies, as well as an option to access the second layer of information and to select or manage cookies. In addition, when the legal basis adopted is consent, there must be a clear and unambiguous option to reject cookies processed on that basis, displayed with equal prominence to the acceptance option, in order to avoid the use of dark patterns.
- In the second layer, accessible from the first, cookies should be organized into categories defined and described according to their purposes, allowing the data subject to enable or disable each category individually. When the legal basis adopted is consent, such categories must remain disabled by default.

4.4 Sensitive Data in Marketing

For information to be considered sensitive personal data, it must fall within the exhaustive list¹⁸ set forth in Article 5, II, of the LGPD. In other words, it must relate to: racial or ethnic origin, religious belief, political opinion, membership in a trade union or in a religious, philosophical, or political organization, data concerning health or sexual life, genetic or biometric data, when linked to a natural person.

¹⁷ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>.

¹⁸ https://processo.stj.jus.br/processo/julgamento/electronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788®istro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF

For businesses, this brings greater predictability: information that does not strictly fall within these categories is treated as ordinary personal data, which may allow the assessment of legitimate interest for campaign optimization and personalization, provided that the legal basis is effectively applicable to the specific case and accompanied by the corresponding balancing test.

Concerns regarding sensitive data arise when the combination of ordinary data allows the inference of a sensitive characteristic¹⁹. However, for such inference to be legally relevant, it must enable the identification or individualization of the data subject from the perspective of that sensitive data.

“When marketing knows about your health before your family” — a paradigmatic case of sensitive personal data processing: based on demographic data analysis and purchase history, a major U.S. retail chain was able to infer that a teenage girl was pregnant (data related to her health) before she had even told her own father, and subsequently began sending coupons and offers targeted at pregnant women²⁰.

As a general rule, the use of such information in marketing requires the data subject’s specific and highlighted consent, segregated from other consents or, at a minimum, the use of mechanisms that clearly highlight the processing of sensitive personal data subject to processing (e.g., specifically and prominently mentioning such data in the layer where the data subject effectively provides consent).

On the other hand, the use of aggregated or statistical data to understand market trends (e.g., an increase in searches for maternity products in a certain region) does not constitute processing of sensitive data, as it does not focus on identifying individual data subjects (anonymized data).

4.5 Consent or Pay

Consent or Pay is an alternative business model that has spread mainly among certain social networks and other “free” services, as a result of restrictions imposed by European data protection supervisory authorities on the use of personal data for targeted advertising.

¹⁹ <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf>

²⁰ <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

In the advertising context, Consent or Pay refers to business models that cumulatively²¹:

Offer the data subject two or more options with the possibility to: • consent to the processing of their personal data, without being required to pay for access to the product or service • choose to pay for access to the product or service, with a consequent reduction in the processing of their personal data	Directs consent specifically toward advertising purposes, especially behavioral advertising (advertising based on profiling the data subject according to their behavior over time, even where combined with data proactively provided by the user themselves).
--	---

The ANPD has not yet taken a position on this model, but the European Data Protection Board (EDPB) addresses it in Opinion No. 08/2024²², in which it presents relevant safeguards to ensure that consent satisfies the validity requirements listed above:

Requirement 1: Freely Given Consent

Existence of a viable alternative to consent:

- ✓ **Provision of a free alternative:** although there is no obligation to offer free services, the availability of an alternative involving a lower degree of personal data processing for advertising purposes, such as the exclusive use of data directly provided by the data subject, tends to reinforce the validity of consent
- ✓ **The amount charged must be reasonable:** the fee must (i) be reasonably necessary; (ii) not make refusal of consent impracticable in practice; and (iii) have its amount determined in a documented manner, in compliance with the accountability principle

Absence of significant detriment to the data subject:

- ✓ **Affordable cost:** the amount charged cannot, in practice, inhibit freedom of choice
- ✓ **Lack of access to the service must not lead to substantial impacts on the data subject's life:** the consent will tend not to be considered freely given if the service (i) is essential or irreplaceable in the data subject's life; (ii) constitutes a practical condition for participation in social life; (iii) prevents access to employment or professional networks; (iv) creates network effects that make refusal of consent impracticable; or (v) generates a lock-in effect due to the user's previously consolidated digital presence

Imbalance of power:

- ✓ **Absence of negative consequences:** in scenarios involving an imbalance of power, consent should only be used insofar as the absence of negative consequences is guaranteed. Examples of indicators of such scenarios include: (i) a dominant market position held by the organization; (ii) services that have built a large user base from an originally free offering; and (iii) processing activities directed at vulnerable audiences

²¹ https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

²² https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

Requirement 2: Informed Consent

In addition to the information required under Brazilian law, the EDPB recommends that data subjects be informed of:

- ✓ Which data is collected regardless of the data subject's choice regarding behavioral advertising
- ✓ The right to withdraw consent and the consequences thereof
- ✓ Any combination or cross-use of data, indicating whether and to what extent the data is shared with other services or controllers

Requirement 3: Unambiguous Consent

Special care must be taken regarding the language used, so that:

- ✓ It is clear for which purpose the data subject is providing consent
- ✓ Consent is not presented merely as an alternative to payment
- ✓ Expressions that emphasize only the gratuitous nature of the service, to the detriment of clearly explaining the data processing resulting from consent, should be avoided

Requirement 4: Specific Consent

The purpose of the processing must be specific, explicit, and legitimate, formulated in such a way as to allow the data subject to clearly understand which processing activities will be carried out based on the consent provided.

5. Targeted Advertising and Profiling

Profiling consists of the systematic analysis of personal data to evaluate, infer, or predict aspects of an individual's personality, behaviour, interests, and habits. It is typically a form of automated processing of personal data that uses such information to analyze or anticipate elements such as professional performance, economic situation, health, preferences, reliability, behaviour, location, preferences, or movements of a natural person²³.

²³ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/>

In the marketing context, profiling is commonly used to:

- Identify consumer preferences, directing advertising for products more closely aligned with their interests
- Predict customer behavior, e.g., identifying likely churn cases to enable preventive action
- Make decisions, e.g., selecting the best advertising strategy for each profile

 ATTENTION!

Advertising segmentation is not necessarily profiling.

Although audience segmentation in advertising campaigns may occur through profiling techniques, such practice is not a necessary requirement for targeted advertising. The mere targeting of advertising based on basic demographic information—such as segmenting consumers by age group, gender, or geographic location—does not, in itself, constitute profiling, insofar as it does not involve the analysis of personal data aimed at evaluating, inferring, or predicting aspects of the data subjects' behavior, personality, or individual preferences.

Where profiling results in a decision based solely on automated processing of personal data and produces legal effects or significant practical impacts on the data subject, **the rights provided for in Article 20 of the LGPD** must be observed. The mere use of profiling for advertising segmentation or personalization purposes, without a significant automated decision concerning the data subject, should not, by itself, be treated as an automatic trigger for the application of art. 20.



²⁴ ICO. **Automated decision-making and profiling**. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/>

Rights under Art. 20

Explanation: possibility of requesting clear and adequate information about the criteria and procedures used in the automated decision, subject to commercial and industrial secrecy.

- Recommendation: the information should include, at a minimum, the personal data used in the creation of the profile and their respective sources (STJ Precedent No. 550²⁵)
- When part of the information is not intelligible to a human person, it may be replaced by clarifications regarding: (a) what the information consists of; (b) why it cannot be provided; and (c) how it is maintained²⁶.

Review: possibility of requesting the review of decisions made in an automated manner, including those based on profiling.

- Currently, there is no legal obligation for such review to be carried out by a human person²⁷, but it is essential that an effective and fair review takes place, capable of changing the outcome of the decision
- Example: allowing the data subject to point out incorrect or outdated information, promoting its correction and the re-execution of the profiling process based on the updated data

Although the LGPD does not expressly state it, it is a reasonable interpretation that the rights described above apply only in situations where automated decision-making produces legal effects or significant practical impacts on the data subject, similarly to the GDPR. Examples in which marketing-related decisions may generate relevant impacts on the data subject include:

- Automated determination of eligibility for offers or benefits
- Profiling that materially or significantly defines the data subject's experience, such as priority support, type of service, access to substantially differentiated offers, or other relevant conditions in the relationship with the brand
- Pricing systems based on profiling (although the legality of such systems is questionable under Brazilian consumer law)
- Approval or automatic exclusion from loyalty or rewards programs

ATTENTION!

Relevant decisions may require the preparation of an Data Protection Impact Report.

When the processing of personal data for automated decision-making purposes generates legal effects or significant practical impacts on the data subject, it is recommended to prepare a Data Protection Impact Report (Relatório de Impacto à Proteção de Dados Pessoais – RIPD). This is because, in such cases, the activity is likely to be considered a high-risk processing operation under Article 4 of ANPD Resolution CD/ANPD No. 2, as it meets a general criterion (potential to significantly affect the interests and fundamental rights of data subjects) and a specific criterion (decisions made solely based on automated processing of personal data).

²⁵ https://arquivocidadao.stj.jus.br/index.php/sumula-550-2;jsad?sf_culture=en

²⁶ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/#access>

²⁷ <https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445>

6. Programmatic advertising and the AdTech ecosystem

Programmatic advertising has revolutionized the industry by enabling the automated purchase of media in milliseconds, ensuring that the right message reaches the right consumer at the ideal moment. The Real-Time Bidding (RTB) model is the cornerstone of this efficiency, optimizing budgets and democratizing access for small advertisers to large advertising inventories.

Typically, the data flow in the programmatic advertising ecosystem operates as follows²⁸:

- A user accesses a publisher's website
- The publisher sends a request to the SSP, sharing any information it holds about the user and the content being viewed
- The SSP sends an ad request to multiple DSPs representing advertisers interested in purchasing ad inventory (the request generally includes user data such as geolocation, IP address, device details, inferred interests (profile), demographic information, and the web application the user is accessing)
- The DSPs automatically analyze the available user data, such as demographic information or browsing behavior, in order to assess the value of that advertising impression. In addition to the data provided by the SSP, this evaluation may rely on user profiles previously built by advertisers
- Based on this analysis, DSPs place automated bids for the available ad inventory
- The SSP conducts a real-time auction and selects the highest winning bid
- The winning advertiser's ad is then displayed on the publisher's website

The entire process takes place in milliseconds and is known as Real-Time Bidding (RTB)

²⁸ <https://www.waytogrow.com/blog/ssp-platforms/>; <https://www.eff.org/deeplinks/2026/01/google-settlement-may-bring-new-privacy-controls-real-time-bidding>

CHALLENGES:

- In the Real-Time Bidding (RTB) model, the information required for audience targeting circulates among multiple actors so that the auction can take place in milliseconds. The market must ensure that this flow is guided by the principle of proportionality, guaranteeing that only the data strictly necessary for the pricing of the impression is shared
- The risk of malicious actors seeking access to data without a genuine intention to purchase media must be addressed through rigorous vetting of technology partners. Advertisers and agencies should prioritize the use of networks and platforms (DSPs and SSPs) that adopt robust security protocols
- When appropriate, evaluate other forms of targeted advertising, such as contextual advertising, in which targeting is not based on the processing of user data but rather on the context of the environment in which the user is located, aligning advertising with the content being accessed—for example, displaying running shoe ads on a page about a road running event²⁹
- Use of walled gardens (closed ecosystems in which operations and data are centralized and controlled by the platform operator), where advertisers' access to user data is limited, which helps protect user privacy compared to the RTB model. However, this model is criticized in marketing due to lower transparency regarding data, metrics, and processes
- Addressing and regulating the relationship between independent controllers involved in the process, such as aggregators and data providers (data brokers), which collect, enrich, and trade databases between advertisers and platforms—ensuring compliance with transparency obligations, legal basis requirements, security, and response to data subject rights

7. International data transfers in marketing³⁰

In digital marketing operations, most international data transfers occur incidentally. This is the case, for example, when:

- The email marketing platform is hosted on servers located abroad
- The CRM uses cloud infrastructure located outside Brazil
- Analytics or programmatic advertising tools operate from foreign data centers

In these cases, the transfer is not the main purpose of the processing activity, but rather a technical consequence of the adopted technological architecture.

²⁹ <https://iabeurope.eu/wp-content/uploads/IAB-Europe-Guide-to-Contextual-Advertising-July-2021.pdf>

³⁰ <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>

For International Data Transfer to be lawful, two requirements must be met:

- It must be based on one of the legal bases set out in Articles 7 and 11 of the LGPD, as applicable
- It must rely on one of the International Data Transfer Mechanisms listed in Article 33 of the LGPD

When the transfer is merely instrumental or secondary, the legal basis supporting the main processing activity (such as legitimate interest or consent) may, as a rule, also support the transfer, provided that the safeguards required by applicable regulations are adopted.

Even so, there remains the obligation to:

- Ensure a valid legal mechanism for the transfer
- Guarantee an adequate level of data protection
- Clearly inform the data subject about the occurrence of international data transfer

A different situation arises when the international transfer itself constitutes a central element of the operation. This may occur, for example, when:

- There is strategic sharing of a database with a foreign headquarters for analytical purposes
- Data is sent to third parties abroad for enrichment, behavioral modeling, or consolidation of global profiles
- The marketing operation is structured based on processing centralized in another country as an essential part of the business model

In such cases, the transfer is a structural part of the processing purpose, and the compatibility of the legal basis used must be assessed with greater rigor.

Once the legal basis is established, it is necessary to evaluate the implementation of international data transfer mechanisms (for example: the hypotheses provided in Article 33 of the LGPD), whose purpose is to ensure that data remains subject to the same level of legal protection even when transferred outside the country.

The Controller only directly implements the international data transfer mechanism when it is responsible for exporting data to a data processing agent located in a third country.

Practical examples	Is the controller the exporter?
The Controller contracts a service that, by its very nature, involves cross-border data flows (e.g., a global cloud processing and data storage network)	✓ Yes
The Controller contracts a national supplier, and the supplier chooses to engage a sub-processor located abroad	✗ No

Therefore, when the Controller acts as the exporter, it is essential that it directly implements the international data transfer mechanism—which, as a rule, will involve requiring the importer to adhere to standard contractual clauses³¹.

When the Controller does not act as the exporter, it must require its supplier to contractually commit to implementing the applicable international data transfer mechanisms and to provide evidence of their effective implementation.

EXCEPTION: transfers to data processing agents located in the European Union, due to the existence of mutual adequacy decisions, are exempt from any additional mechanisms.



NOTE

When the international data transfer mechanism has a contractual nature, the Data Subject has the right to request a copy of the relevant contractual clauses, safeguarding any trade secret elements contained therein. Therefore, it is essential that the Controller retains a copy of the applicable clauses. In addition, the Controller is responsible for providing information regarding international data transfers, as already addressed in the transparency section.

8. Children and adolescents in digital marketing

Law No. 15,211/2025 (Digital Child and Adolescent Statute), interpreted in conjunction with the LGPD, reinforces the protection of children and adolescents in the digital environment and establishes stricter parameters for the processing of their personal data in the advertising context.

The full protection of this group requires that digital marketing strategies be structured with enhanced governance, necessity criteria, and preventive risk mechanisms.

³¹ <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>

a) Legal basis for processing minors' data:

The processing of personal data of children and adolescents may be carried out based on the legal grounds provided for in art. 7 or art. 11 of the LGPD, provided that their best interests are observed and prevail, to be assessed on a case-by-case basis, pursuant to art. 14 of the Law, as stated in CD/ANPD Statement 1/2023.

Legitimate interest: although its use is legally possible, it must always comply with the principle of the best interests of the child and adolescent.

ATTENTION!

Consent for the processing of children's personal data must be given by parents or legal guardians, as provided by the LGPD. With regard to adolescents aged 16 to 18, who have limited legal capacity under Brazilian law, it is recommended that at least parental or guardian assistance be ensured.

b) Best interests of children and adolescents:

The best-interests principle encompasses three dimensions³²:

- **Substantive right:** ensuring that the child's best interests are primarily considered in any decision affecting them, individually or collectively
- **Principle:** requiring that, where multiple interpretations of a rule are possible, the one that best serves the child's interests must prevail
- **Procedural rule:** requiring that decisions impacting children include an assessment of their effects, with procedural safeguards and explicit justification of how the best interests were considered

The main point is that the strategy must not instrumentalize vulnerability as a competitive advantage.

- **Example:** processing personal data for targeting books and other age-appropriate educational content is appropriate. On the other hand, any form of targeted advertising based on profiling is prohibited under the Digital Child and Adolescent Statute (ECA Digital)

In any case, it is always important to document the assessment process of the child's best interests.

³² https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf

c) Risk management:

The ECA Digital establishes that whenever providers of information technology products or services process personal data of minors for purposes other than the mere operation of the product or service, they must carry out risk management activities, including at least: (a) mapping and mitigating the risks involved; and (b) preparing a data protection impact assessment.

d) Profiling:

Profiling is a technique that has been widely used in recent years as a marketing strategy, as it allows a deeper understanding of the customer and optimizes marketing campaigns by enabling the delivery of the right (and personalized) message to the intended audience. Through the collection and analysis of personal data, it identifies characteristics, behaviors, interests, and needs, resulting in the construction of detailed profiles for each individual, enabling individualization and the creation of more personalized and effective marketing strategies.

According to the consolidated understanding of the Digital Child and Adolescent Statute, profiling techniques, when directed at minors (who are more susceptible to suggestion), have a greater potential to exploit the psychological vulnerability of this audience, who, in line with the Federal Constitution and the Child and Adolescent Statute (ECA), are considered individuals in a special stage of development without sufficient discernment to understand data-driven digital marketing strategies. **For this reason, the law prohibits profiling and emotional analysis of children and adolescents for the purpose of targeting commercial advertising to this audience.**

Thus, when designing campaigns with profiling strategies for advertising targeting, brands and agencies must now adopt strict guidelines, not only avoiding any use of personal data that involves the identification or segmentation of minors, but also implementing effective safeguards to exclude underage individuals from such practices.

IMPORTANT!

The mere existence of advertising segmentation or profiling itself does not imply a violation of the Digital Child and Adolescent Statute or the LGPD. The following remain legally permissible and often necessary: broad segmentation by age group; age-appropriate content classification; safety filters; age verification tools; and contextual communication not based on individual tracking. In fact, the responsible and ethical use of personal data is a prerequisite for enabling the full protection of children and adolescents.

To mitigate the risks of conducting advertising profiling involving minors, it is important to adopt specific measures in the development of age-restricted campaigns, such as³³:

- ✓ Avoid using media with a significant volume of minors (e.g., more than 25% of the audience), including analyzing demographic data of influencers' followers before partnerships
- ✓ Use available technology to ensure that ads are negatively targeted at this audience, so that minors do not receive the advertising content (e.g., negative targeting, age-gating)
- ✓ Avoid the use of lookalike audiences / automatic audience expansion when there is a risk of reaching minors: these techniques automatically expand targeting to users "similar" to the original audience (based on behavior patterns, interests, or profiles), which may inadvertently include minors—especially when the source data is not fully reliable or when there is overlap between adult and youth interests. In such cases, it is recommended to disable this type of automatic optimization or use it only with additional restriction layers (e.g., robust age exclusions and clearly adult interest filters)
- ✓ Evaluate the age-restriction advertising policies of the platform to be used

In addition, when entering into contracts with advertising agencies and other entities involved in the marketing chain, it is important to establish contractual obligations regarding the adoption of appropriate measures to prevent advertising profiling of minors.

e) Age verification:

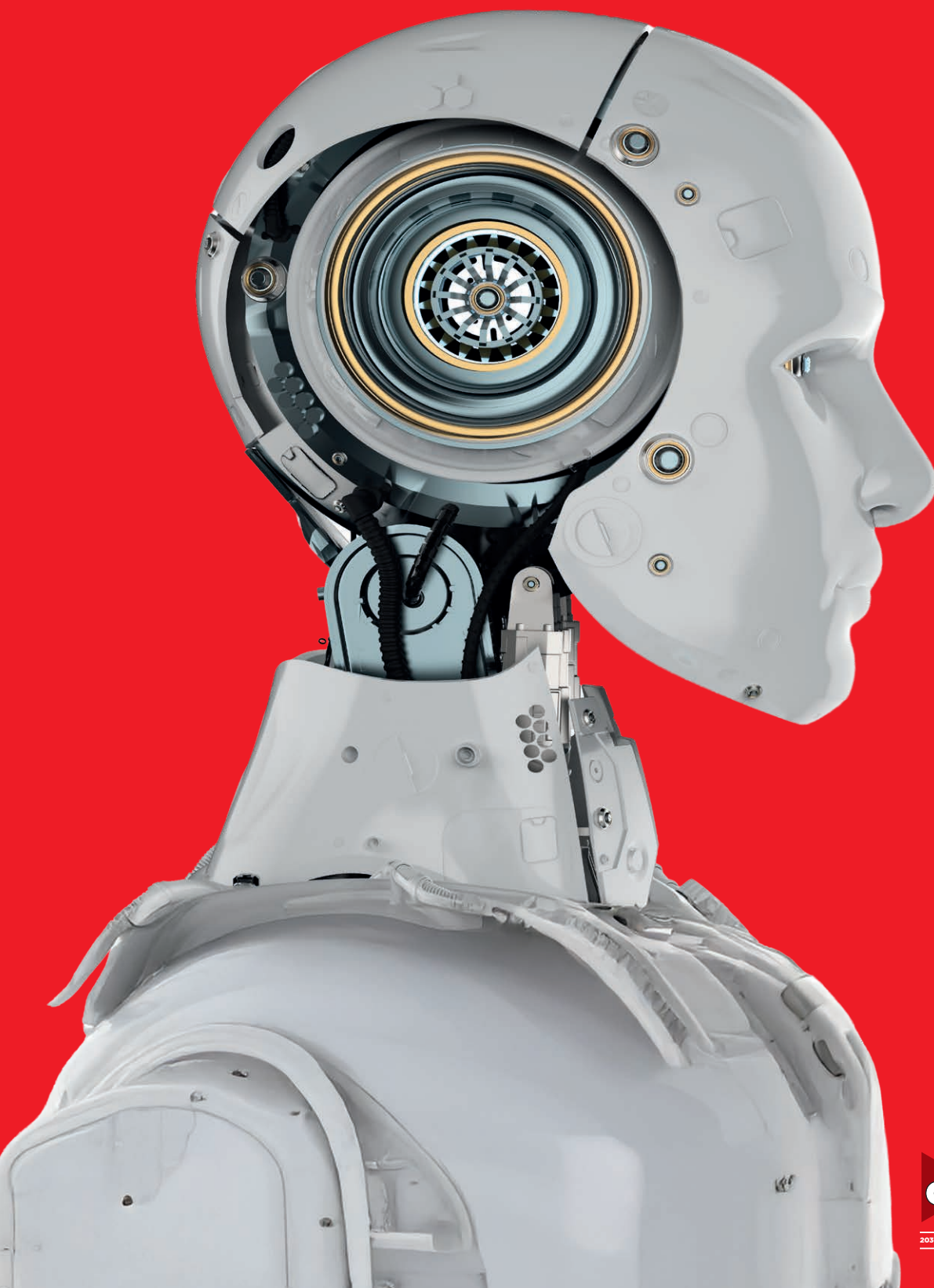
To comply with regulatory obligations, especially those provided for under the ECA Digital, it will be necessary to adopt age verification mechanisms - i.e., mechanisms that allow the user's age to be confirmed and ensure compliance with the rules applicable to the processing of children's personal data.

Such mechanisms must be implemented in a risk-proportionate manner, prioritizing approaches that minimize the additional collection of personal data. In addition, it is important to note that the ECA Digital prohibits the use of personal data collected for age verification purposes for any other purpose.

³³ <https://www.asa.org.uk/static/44dc1935-0766-4378-91171e6954ae560a/Age-restricted-ads-online-targeting-guidance.pdf>

▶▶ CHAPTER II

Artificial Intelligence in Marketing



1. “Traditional” AI vs. Generative AI in marketing

In a broad sense, artificial intelligence (AI) can be understood as a set of computational techniques and models designed to, based on data and other inputs, identify patterns, estimate probabilities, generate recommendations, classify information, or support decision-making, in accordance with defined objectives and parameters.

In marketing and advertising, AI models have been used for years, for example, for audience segmentation, ad personalization, consumer behavior prediction, recommendations, media optimization, and performance measurement. These models are often integrated into or “embedded” within platforms and tools, operating through the analysis of usage data, telemetry, derived signals, and performance metrics (such as impressions, clicks, time on page, conversion events, frequency, viewability, ad context, and aggregated outcomes) to continuously adjust decisions such as delivery, bidding, and creative prioritization.

Generative AI, in turn, is a subcategory focused on creating original content from patterns learned from large volumes of data. Generative AI produces text, images, videos, audio, or code; can operate in a conversational format; adapts its outputs according to context and received instructions (prompts); and enables dynamic interaction with users.

2. Where AI fits into the advertising value chain

AI is deeply integrated into all stages of the marketing journey, transforming the way ads are conceived, created, targeted, and delivered. Its application is not limited to a single function, but spans the entire workflow, from strategic planning to results measurement. It may be visible (when a team uses a generative tool to create assets) or invisible / “embedded” (when platforms apply models to rank content, optimize bids, distribute ads, and measure outcomes).

This creates opportunities for gains in productivity and quality, but also increases legal, reputational, and operational risks, especially when usage occurs at scale and with low traceability³⁴. Therefore, the starting point of this Good Practices Guide is to map where AI appears, who controls each decision, and what evidence must exist to support compliance and trust.

Planning, Insights, and Innovation

- **Predictive Analytics:** Uses machine learning algorithms to forecast consumer behavior and campaign performance even before launch

³⁴ https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20%26%20challenges%20in%20generative%20AI.pdf; https://iabbrasil.com.br/wp-content/uploads/2024/11/IAB_Guia_de_Uso_da_Inteligencia_Artificial_na_Publicidade_Digital_nov24_AF.pdf

- **Insight Generation:** Analyzes massive volumes of structured and unstructured data to identify patterns, trends, and new business opportunities
- **Product Innovation:** Uses AI-generated insights to optimize product development and user experience design based on real user needs

Content Creation and Production

- **Multimodal Generation:** Creation of texts (copy), photorealistic images, camera-free videos, audio, and soundtracks based on prompts
- **Dynamic Content:** AI tools generate ad variations in real time, adapting messages and offers to each consumer's individual preferences
- **Creative Ideation:** Supports brainstorming and campaign development processes, enabling exploration of new creative directions

Media, Targeting, and Delivery

- **Programmatic Advertising:** Algorithms automate the buying and selling of ad inventory, optimizing bidding and budget allocation in milliseconds
- **Profiling and Micro-segmentation:** Uses deep learning to build complex behavioral profiles, enabling highly specific targeting based on habits and preference
- **Campaign Optimization:** Applies reinforcement learning to continuously improve ad performance, adjusting delivery parameters in real time

Customer Activation and Relationship Management

- **Chatbots and Virtual Assistants:** Use of Natural Language Processing (NLP) enables instant, personalized support capable of simulating human-like empathy
- **Customer Experience (CX) Personalization:** Analyzes purchase history and browsing data to offer tailored product and service recommendations

Measurement and Outcomes

- **Attribution and ROI:** Helps identify which channels and messages deliver the best return on investment, enabling data-driven decision-making
- **Brand Monitoring (Brand Safety):** AI tools perform real-time audits to ensure ads are not displayed alongside inappropriate or fraudulent content

2.1 Chain actors: who does what and where AI typically enters

To facilitate understanding, the advertising chain can be grouped into four core pillars. For governance purposes, it is important to understand where automated decision-making occurs, who controls the process, and who retains evidence³⁵.

³⁵ <https://aba.com.br/wp-content/uploads/2025/10/ChecklistADIGITAL.pdf>; <https://iabbrasil.com.br/wp-content/uploads/2024/11/Guia-do-uso-de-IA-na-publicidade-digital.pdf>; https://drive.google.com/file/d/1_F4eGbP_HixRSks2SXNZS_LUR0MrZ0Fb/view

ADVERTISING VALUE CHAIN WITH AI: WHERE IT APPEARS

Actor	AI presence	Decisions
Advertiser	Approval of AI-generated creative; personalization; customer service; measurement	Defines guidelines, approves the creative, and “goes live”
Agency	Creation of assets, variations, storyboards; automation; use of APIs/models	Selects tools, operates prompts, composes materials
Platforms/ Publishers	Recommendation/ ranking; segmentation; delivery optimization	Defines system parameters; advertiser defines objective and audience
AI Providers	Generation and editing tools; general-purpose models	Provider: defines architecture; client: use and inputs
Production Providers	Image/ voice banks; studios; freelancers	May incorporate third-party inputs
Consumer/ Audience	<i>AI-driven chatbots and experiences; synthetic content</i>	May interact with AI, inducing errors or misleading outputs

2.2. AI as a tool, creative partner, and legal risk

A practical way to understand the impact of AI in the chain is to distinguish three modes of use:

(i) AI as a tool (“copilot”)

AI acts as operational support: it speeds up tasks, suggests alternatives, and automates repetitive steps. Humans tend to retain direct control over the output, but review and traceability are still essential, because speed and scale amplify errors and violations.

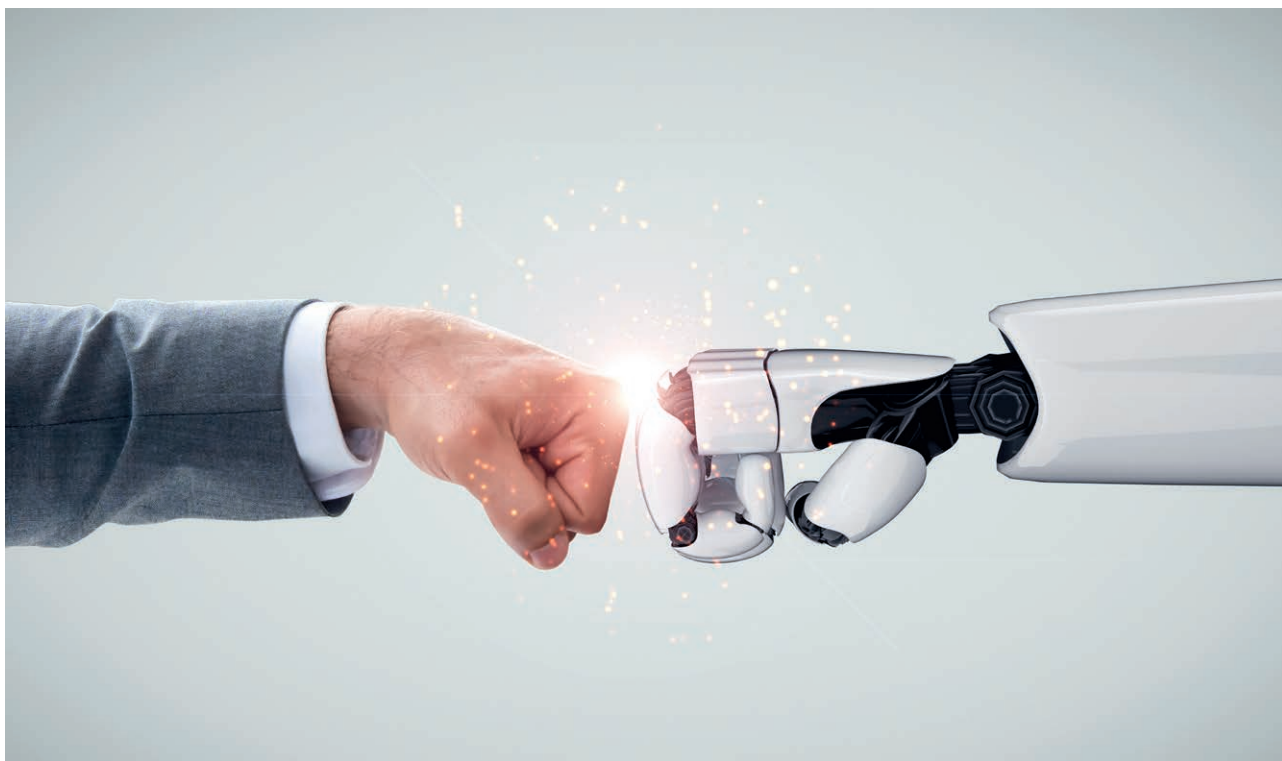
(ii) AI as a creative partner (“co-creation”)

AI begins to influence creative choices, generating images, scripts, voices, scenes, and variations at scale. This mode brings productivity gains and new possibilities for expression, but increases risks of misleading synthetic content, copyright infringement, and unauthorized use of image/ voice. Therefore, governance must treat outputs as advertising content subject to standards of truthfulness, accountability, and diligence.

(iii) AI as an “embedded” legal risk

AI operates “behind the scenes,” in the “backstage,” within platforms and providers, in ranking, recommendation, targeting, bidding, attribution, and moderation. The risk here is twofold: opacity (difficulty in explaining why a decision was made) and indirect impact on consumers (e.g., inappropriate targeting, discrimination, exposure to manipulated content, and persuasive pressure)³⁶.

³⁶ https://drive.google.com/file/d/1_F4eGbP_HixRSks2SXNZS_LUR0MrZ0Fb/view; https://iabbrasil.com.br/wp-content/uploads/2024/11/IAB_Guia_de_Uso_da_Inteligencia_Artificial_na_Publicidade_Digital_nov24_AF.pdf



2.3 Responsibility across the chain

When artificial intelligence becomes part of the creative and operational marketing chain, it directly impacts already regulated and sensitive dimensions of advertising activity, such as truthfulness of information, prohibition of misleading or abusive advertising, transparency, consumer protection, copyright and personality rights, non-discrimination, and information security.

The use of AI does not create a regulatory “exception zone.” Legal and self-regulatory obligations remain fully applicable, including in cases involving:

- Commercial claims related to the use of AI (technological claims)
- Synthetic content that may create confusion regarding authenticity, under penalty of being considered misleading or abusive to consumer trust³⁷

In addition, the more AI becomes conversational (assistants, chatbots, avatars) and the more it “personalizes” decisions (segmentation/optimization), the higher the risk of material confusion, undue trust induction, and relevant impacts on consumers. In such cases, transparency, disclosure, and clear definition of responsibilities are no longer optional safeguards. It is therefore important to treat transparency and disclosure as part of campaign design, while avoiding label fatigue³⁸.

³⁷ In this regard: https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; <https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html>; <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>; https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust/

³⁸ <https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/>

LABEL FATIGUE and when to include DISCLOSURE

To reduce label fatigue without losing trust, the recommended approach is based on materiality.

The use of disclosure is:

- more important when AI may alter the consumer’s perception of authenticity, identity, or representation (e.g., synthetic person/voice/performer, realistic synthetic scenes, simulated testimonials/experiences), influencing the understanding of the product or service offered and potentially impacting purchasing decisions and/or choice
- less relevant when AI operates as a back-end tool with no material risk of deception

Given the lack of regulatory and self-regulatory consensus on a general rule for labeling AI-generated or AI-assisted content, the decision on disclosure should remain tied to the materiality of the risk of deception, confusion, or undue consumer influence.



IMPORTANT NOTE!

As AI-generated and synthetic content scales, demand for consistent transparency and clear disclosure criteria (“when” and “how” to inform users) increases. Although, transparency and labeling may strengthen trust, they do not replace compliance (nor do they “shield” a campaign from challenges related to misleadingness, abuse, or unfair practices)³⁹.

WHAT IS EXPECTED FROM EACH ACTOR IN THE CHAIN?

Actor	What is expected	Where responsibility ends	How to address internally (contract/ process)
Advertiser (Brand)	Define risk limits and levels; approve the use of AI and tools; require human review before the use of generated outputs; define when disclosure will be required; establish correction/removal and incident response plans; prohibit the use of the advertiser’s information for training AI systems; and set out in contracts with the agency all intellectual property rules applicable to AI-generated deliverables	Remains the primary party responsible to the public for the piece/claim/ disclosure	Internal policies; structuring robust contracts with agencies; prior approval of tools; review and approval workflows; requirements for traceability and SLAs

³⁹ <https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/>; <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>; <https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html>

Actor	What is expected	Where responsibility ends	How to address internally (contract/process)
Agency	Inform, document, and disclose AI use; use only approved tools; maintain traceability (date, prompt, logs, model version); fact-check and assess legal risks; obtain/confirm rights; notify subcontracting where contractually permitted	May share responsibility when creating/controlling content on behalf of the advertiser, but does not replace final responsibility towards the public/consumer	Obligations include prior notification, documentation, human review, traceability, and advertiser approval before publication, as well as contractual clauses on liability for inputs and outputs, including representations and warranties regarding third-party rights, indemnification obligations, and liability for incorrect, harmful, or non-compliant outputs
Suppliers	Minimum transparency on functionality and limitations; security and confidentiality; clear options regarding data retention/training; support for logs and auditing; prompt incident notification	Typically has no direct relationship with the consumer, but may generate operational and legal harm; nevertheless, advertising remains attributable to the Advertiser/Agency	SLAs, obligation to notify incidents, right to audit and assess controls, and requirement that subcontractors comply with equivalent standards
Platforms (Publishers)	Enforcement of ecosystem policies; labeling mechanisms when available; ability to reject/flag ads	Do not assume the Advertiser's accountability; platform-applied labels may complement, but do not replace it	Prefer disclosure integrated into the creative/ad material itself; even if the label is applied by the platform, the Advertiser remains responsible for ensuring the adequacy of the disclosure

CONCLUSION

The primary responsibility for deciding whether AI disclosure/labeling is required (and how this information will be presented) generally lies with the Advertiser (brand) or with the Agency that creates and controls the content on behalf of the Advertiser. Platforms, in turn, apply their own rules and moderation/labeling mechanisms within the environment where the ad is displayed, but this does not transfer or replace the advertiser's responsibility for compliance and transparency in communication.

▶▶ 3. Real-world use cases of AI in marketing

Within the advertising value chain, AI is used both in behind-the-scenes activities (analysis, automation, and optimization) and in outputs that directly affect consumers (advertising materials, claims, and customer service).

AI (especially generative AI) is already widely used by professionals to shorten production cycles, support creation, and automate tasks. It can assist from the generation of creatives and variations to media planning, insight extraction, and customer service responses. At the same time, quality can be variable, and human review is essential to ensure adequacy and prevent risks.

Rule of thumb: anything intended for public use (or that influences relevant marketing decisions) must undergo **human review** and have **traceability** (e.g., prompt/log/model/version/who approved it).

OVERVIEW: WHERE AI TYPICALLY ENTERS (FROM CREATION TO POST-CAMPAIGN)

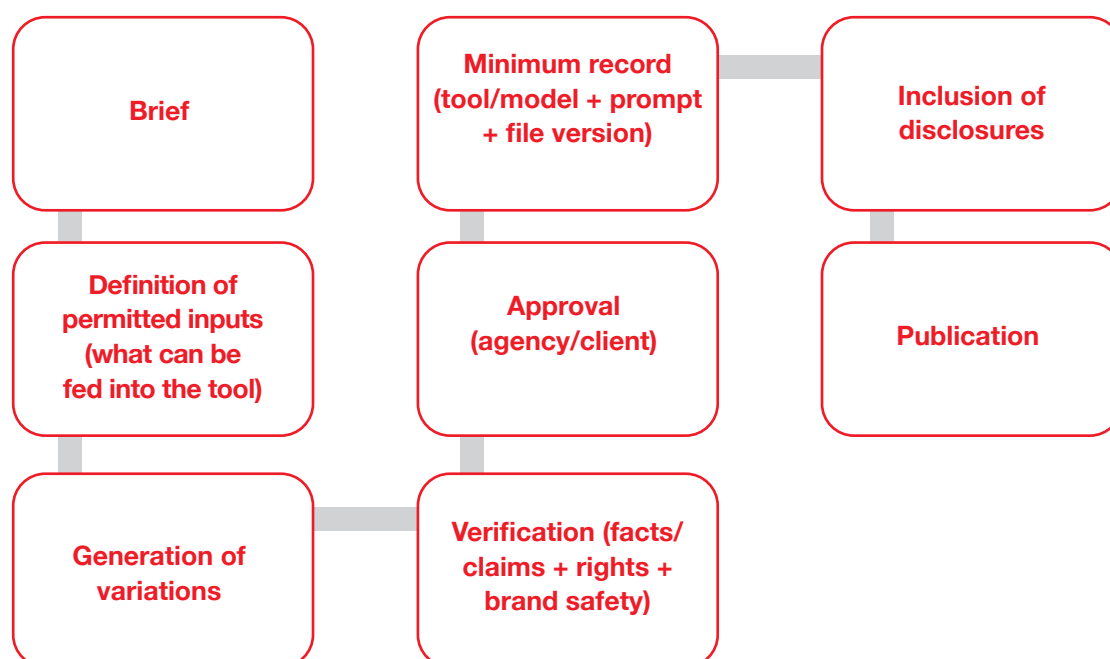
Stage	What AI typically does	Practical examples	Typical risks	Quick safeguards
Strategy and briefing	Organize inputs, map audiences and hypotheses	Summarize insights; suggest messaging; prioritize tests	Biases; hallucinations; decisions without basis	Human review and source validation (do's & don'ts)
Content production	Accelerate creation and variations	Texts, images, scripts, A/B versions	Intellectual Property issues, personality rights; misleading content	Human review; checks; traceability
Media and optimization	Support segmentation, buying and adjustments	Pacing; bidding; performance-based allocation	Discrimination; opacity	Auditing and transparency; documentation
Measurement and attribution	Model impact and estimate contribution	Models, signal interpretation, dashboards	Confusion between correlation and causation ("cause and effect") and overclaiming	Testing, validation, governance, and decision trail
Customer service and research	Automate interactions and insights	Chatbots; feedback summaries; research; synthetic personas for insights	Incorrect responses; prompt injection (attempts to manipulate the model)	Supervision; testing; resilience mechanisms

3.1 Content creation (text, image, video, audio, and variations)

Generative AI and related tools are used for ideation, production, and adaptation of assets at greater speed and scale (headlines, slogans, posts, product descriptions, voiceovers, scripts, and creative variations). In the context of digital advertising, use also extends to reference images (moodboards, storyboards), campaign visuals, illustrations, photorealism, and editing/adjustments (removal/addition of elements, background changes, generative fill).

WHAT TO DO	WHAT NOT TO DO
✓ Ensure human review before publication, including prior advertiser approval for content intended for distribution, especially for facts, comparisons, promises, sensitive topics, health/finance, IP rights, and use of image/voice ✓ Train the team and establish internal safe-use guidelines ✓ Require traceability (prompt/log/model/version) and approval records ✓ Conduct a rights check (copyright, intellectual property, image and voice rights) and keep evidence of authorization when applicable	✗ Publishing or reusing output without human review ✗ Failing to train users who work with AI in their daily activities ✗ Producing content without a minimum traceability trail (no prompt/log/version) ✗ Do not use AI to create “evidence” or simulated “testimonials” that could mislead the public about authenticity (deepfakes/reenactments) without safeguards and transparency when applicable

OPERATIONAL FLOW MODEL



Example prompt with “guardrails”

“Create 10 variations of headlines and descriptions for an ad for [product], ensuring: (i) tone [X], (ii) no absolute claims (‘guaranteed’, ‘100%’), (iii) no comparisons with competitors, (iv) no mentions of sensitive attributes, (v) include 2 more conservative options for compliance. At the end, list which statements require factual verification.”

3.2. Media and optimization (buying, targeting, bidding, and real-time decision-making)

In media and optimization, AI is used to automate decisions that were previously operational and manual, such as bidding, inventory selection, targeting, budget pacing, and creative optimization. These systems process large volumes of signals (user context, aggregated behavior, historical performance, ad environment, time/device, etc.) and make dynamic adjustments to achieve defined objectives (reach, CPA – Cost per Acquisition, ROAS – Return on Ad Spend, leads, sales).

In practice, AI acts as an autopilot that makes micro-decisions at each impression: which ad to show, to whom, when, in which placement, and at what price. This enables efficiency gains and scale, but also introduces a key concern, as decisions become less intuitive and harder to explain, since optimization is driven by models that continuously adjust delivery.

Thus, the risk is not limited to content creation, but also extends to how campaigns are distributed and refined, including impacts on exclusions, vulnerable audiences, brand safety, and potential segmentation biases.



WHAT TO DO	WHAT NOT TO DO
✓ Define guardrails before enabling automation: campaign objective, quality KPIs (not only volume), budget, optimization window, frequency caps, exclusions, and brand safety criteria ✓ Establish clear limits for targeting and exclusions (including preventing impact on children and vulnerable groups, when applicable—for example, adult products on children’s content pages), and periodically review whether delivery complies with the defined rules ✓ Ensure human oversight as part of routine operations: set a minimum monitoring cadence (e.g., daily at the beginning and after major adjustments; weekly in stable operation) to check anomalies, performance drift, and unintended optimization effects ✓ Record relevant decisions and changes: modifications to objectives, audiences, exclusions, creatives, bids, budget, attribution window, and automation settings. This is essential to explain results and support diligence ✓ Maintain a responsibility trail: who approved the media strategy, who executed changes, who reviewed them, and what the rationale was, especially when an agency manages the account and activates automations ✓ Include a contingency (fallback) plan: if automation starts producing anomalous results, define triggers for pausing, rolling back to previous configurations, and rapid escalation	✗ Do not treat automated optimization as a “hands-off autopilot”: automation without oversight and evidence increases the risk of inappropriate delivery, bias, and reputational exposure ✗ Do not optimize only for “easy” metrics (clicks, views, raw leads) without quality indicators and validation; this tends to drive decisions that maximize volume but reduce real value and may encourage questionable practices ✗ Do not allow continuous changes without logging (“invisible adjustments”) — this undermines explainability, auditability, and the ability to correct course when something goes wrong ✗ Do not use automatic targeting/expansion without limits when there is a risk of reaching inappropriate or sensitive audiences; “audience expansion” without guardrails increases the risk of context errors and unintended exposure ✗ Do not rely exclusively on platform labels/rules as a substitute for governance: platform rules help, but do not remove the responsibility of the advertiser/agency for how campaigns are configured and optimized ✗ Do not ignore anomaly signals (sudden spikes, sharp drops in CPA with worse quality, unexplained shifts, concentration in suspicious inventory). In automated media, these “anomalies” are exactly the type of risk that requires pause and review

3.3. Measurement and attribution

Measurement and attribution, in a marketing context, bring together methodologies to quantify the impact of marketing initiatives and assign part of the results (sales, leads, qualified traffic) to different channels and actions. With the advancement of AI, this work has come to combine traditional models with machine learning techniques to integrate multiple sources (media, CRM, website/app, retail, context), reduce noise, and produce more actionable insights, such as estimates of contribution by channel, performance forecasts, and budget reallocation recommendations.

AI generally comes in to: (i) organize large volumes of signals, (ii) detect patterns (e.g., seasonality, response to price/promotion), (iii) forecast performance, and (iv) generate actionable insights — provided there is proper validation, governance, and documentation. The key point is that attribution is not an “exact account,” but an inference based on data and assumptions; therefore, it requires methodological transparency, validation, and documentation.

WHAT TO DO	WHAT NOT TO DO
✔ Treat “AI insight” as a testable hypothesis, validated with context and methodology, not as automatic truth ✔ Document methodology, limitations, and changes (e.g., window, variables, assumptions) to enable auditing and historical comparison	✘ Do not confuse correlation (statistical associations found in data — e.g., “Users exposed to the ad converted more”) with causation when justifying budget, targeting, or performance claims, since the observed lift may be driven by other factors not captured by the AI correlation ✘ Do not “optimize measurement” to make results look better: selecting easy metrics (e.g., clicks) or weak events to inflate performance tends to distort decisions and may lead to misleading claims

3.4 Customer service and research (chatbots, agents, and market research)

AI can generate immediate and personalized responses in customer service, including in multiple languages, and in some cases emulate human characteristics such as empathy. At the same time, it is increasingly being used in research for information synthesis, the analysis of large volumes of data, and support for generating insights.

WHAT TO DO	WHAT NOT TO DO
✔ Make the assistant’s role explicit: communicate that it is an automated solution when relevant to avoid material confusion, especially in more “humanized” interactions (chat/voice/avatar) and in longer engagements ✔ Define a “single source of truth” for responses: limit what the agent can state to official sources (return policies, conditions, prices, timelines, terms), and keep these sources updated with governance (owner + version) to reduce outdated responses	✘ Do not design chatbots/assistants to induce undue trust (“I am an expert”, “I guarantee”, “it is 100% safe”) — this creates risk of misleading practices and reputational harm ✘ Do not allow the assistant to “make things up” (hallucinate) to respond quickly: incorrect answers in customer service can become unintended promises and cause reputational damage ✘ Do not present a chatbot/assistant as a human or as an “authority” when it is not; this increases the risk of undue trust and consumer frustration⁴⁰

⁴⁰ https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust?utm_source=govdelivery

WHAT TO DO	WHAT NOT TO DO
✓ Implement human escalation (handoff) with objective triggers: define clear rules for transferring to human support (e.g., serious complaints, cancellations, billing issues, disputes, fraud, sensitive personal data, children/vulnerable users, regulated topics) and log the reason for the handoff ✓ Use content and tone guardrails: set limits to prevent promises, unwarranted guarantees, aggressive language, or excessive persuasion — and to block recommendations that conflict with commercial policy or transparency obligations	✗ Do not allow the bot to make sensitive factual claims without a defined source (price, deadlines, coverage, contractual terms, policies), especially when the response could be interpreted as a binding commitment from the company ✗ Do not use automated customer service to push consumer decisions in a manipulative way (pressure tactics, artificial urgency, exploitation of vulnerabilities) or for hidden nudge

4. Principles that should govern Responsible and Ethical AI in Marketing

The principles below function as criteria for deciding when to use AI, how to design campaigns, and which controls to require across the chain (Advertiser, Agency, Platforms, and Providers). They reflect convergences between Brazilian and international industry materials, with an emphasis on consumer protection, integrity of commercial communication, risk mitigation, and governance.

4.1. Legitimate purpose and business alignment

The use of AI must be connected to a clear business objective, with defined scope and boundaries (what will be automated, what requires human creation, and what is prohibited). The purpose must be compatible with the campaign context and with audience expectations.

AI usage should begin with the question “what for?”, seeking to assess which legitimate objective it helps achieve (efficiency, scale, quality, responsible personalization, insights), and what limits are necessary to prevent the technology from creating disproportionate risk.

International materials aimed at advertisers reinforce the logic of: pre-defining where AI can be applied, which cases should be avoided, and which minimum controls accompany each use⁴¹. Legitimate purpose also means avoiding “decorative” uses (e.g., AI washing) and focusing efforts where AI improves the process without compromising truthfulness, transparency, and trust⁴².

⁴¹ https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20&%20challenges%20in%20generative%20AI.pdf

⁴² <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>

4.2. Transparency and risk-proportionate explainability

Transparency and explainability underpin trust in the use of AI in marketing, as they enable consumers, clients, and partners to understand when relevant automation is involved, make informed choices, and, when necessary, question or challenge decisions and communications. Although complementary, these concepts are not the same: transparency relates to the duty to clearly inform; explainability refers to the ability to understand and assess, to an appropriate extent, how AI was used and which relevant factors influenced the outcome.

In the case of **transparency**, it is useful to distinguish two complementary dimensions:

(i) Transparency regarding processing and automation: this involves clearly and understandably communicating whether, when, and to what extent AI, automation, or data processing were used, whenever this information is relevant for the understanding of the audience, the client, or partners in the value chain. This includes, depending on the context, information about personal data processing, the existence of relevant automation, the nature of automated interactions, and other elements whose omission could compromise data subject rights or mislead consumers. In this dimension, the transparency and information obligations established under the LGPD are especially relevant, particularly when there is personal data processing, profiling, or automation-supported decision-making. When AI meaningfully influences the creation, personalization, delivery, or evaluation of content, offers, or interactions, such transparency must be accompanied by risk-proportionate explainability tailored to the specific case

(ii) Transparency regarding the nature of communication: this refers to clarity, honesty, and intelligibility of the message in the audience's actual experience. It aims to prevent material confusion or consumer deception regarding authenticity, authorship, human endorsement, advertising intent, or the synthetic nature of content and interactions. This dimension becomes particularly sensitive when the use of AI can significantly alter the audience's perception of the origin, technological mediation, or presentation of the communication. In this context, the duties of clarity, non-deceptiveness, and non-misleading communication under the Brazilian Consumer Protection Code (CDC) are especially relevant, without prejudice to other applicable legal and self-regulatory frameworks, such as the CBAP

In this first dimension, **explainability** does not mean “opening the code” or disclosing model secrets. It means ensuring, when necessary, a sufficient and proportionate explanation of relevant aspects of AI use, such as: what type of automation occurred and for what purpose; which data/inputs were used at an appropriate level of detail; what known limitations exist (e.g., risk of error/hallucination, bias, contextual dependency); and which controls were applied (e.g., human review, fact-checking, filters, audits).

In the advertising field, these principles are especially important because AI can simulate human authorship, generate highly realistic synthetic content, and personalize interactions at scale, which increases the risk of material confusion and misleading users if there is insufficient clarity about the use of the technology⁴³.

The foundation is the same as the self-regulatory framework established by the CONAR Advertising Code: communications must be honest, verifiable, and not misleading. In this context, transparency and explainability function as instruments to preserve trust and accountability, without replacing other compliance duties (e.g., truthfulness of claims, consumer protection, and non-discrimination).

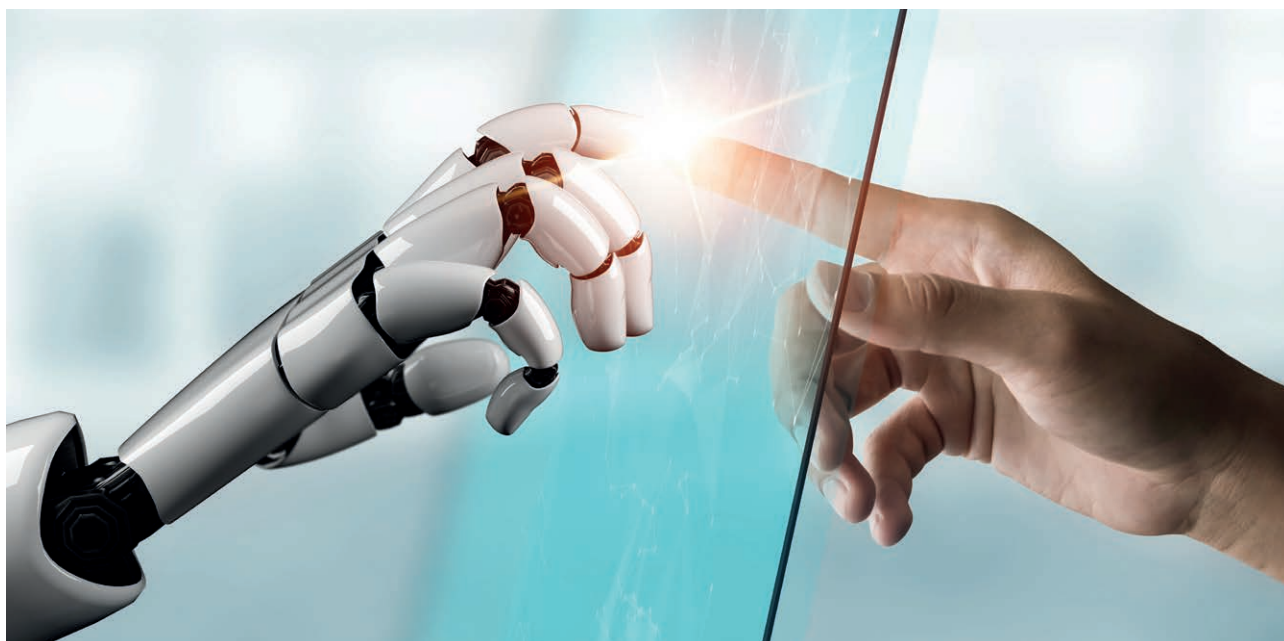
4.3. Human centrality and supervision

AI accelerates workflows but does not replace human accountability, especially when outputs may impact consumers (e.g., claims, recommendations, customer service) or when automation influences or makes decisions with significant impact (e.g., targeting, optimization, attribution).

Sector principles for generative AI in advertising emphasize that there must be a human owner, approval checkpoints, and mechanisms that allow correction before and after publication.

Human supervision is what transforms AI from an “efficient” tool into a “reliable” one, including, depending on the case: fact/claim verification, language review, suitability for sensitive audiences, validation of copyright and image rights, and review of higher-impact automated decisions.

However, human centrality does not require the same level of intervention across all uses; it should be calibrated proportionally to risk, potential impact, and the system’s level of autonomy.



⁴³ https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; <https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/>

It is important, in this context, to distinguish between two scenarios:

(i) AI as a support tool: when AI is used for brainstorming, organizing inputs, generating drafts, creative variations, summarization, analytical support, or recommendation of pathways, without independently producing a final decision with relevant effects for the data subject or consumer. In these cases, human oversight must exist, but it can be organized through sampling-based review, stage approvals, guardrails, checklists, and periodic monitoring, without requiring continuous or fully individualized human review of every low-risk interaction or output

(ii) AI in automated decision-making with relevant effects: when automation materially influences or determines eligibility for offers or benefits, the user experience, pricing, service prioritization, or other decisions capable of producing legal effects or significant practical impacts on the data subject or consumer. In these cases, stronger controls are required, including greater traceability, clear escalation criteria, appropriate transparency, and effective mechanisms for contestation and review. Additionally, in high-risk AI use cases, it is recommended to consider the development of an Algorithmic Impact Assessment (AIA) as a good governance practice for risk mitigation and documentation, inspired by international references and ongoing regulatory discussions in Brazil. Given the current state of Brazilian law, AIA does not constitute a general explicit legal obligation for AI use in marketing, without prejudice to specific obligations that may arise from sectoral regulation, contractual arrangements, platform policies, or the territorial application of foreign rules⁴⁴

In summary, low-risk uses may be governed through predefined controls, usage rules, periodic oversight, and approval trails; higher-risk or high-impact uses require reinforced human intervention, with real capacity to review and correct outcomes and, when characterized as high risk, may justify an AIA as a governance and risk documentation best practice.

4.4. Non-discrimination, fairness, and bias mitigation

AI can reproduce and amplify biases present in data, consumption patterns, and in the way the model has “learned” about the world. In marketing, this manifests in two ways:

- in **content** (stereotyped representations, discriminatory language)
- in **content distribution** (targeting and optimization that unjustifiably exclude groups or reinforce inequalities)

In this context, non-discrimination, fairness, and bias mitigation are essential principles of trust and responsibility. Sectoral and international materials on AI in advertising treat diversity and fairness as pillars, emphasizing human review, testing, and guardrails prior to deployment⁴⁵.

⁴⁴ https://vklaw.com.br/wp-content/uploads/2025/12/VLK_O-Papel-do-DPO_2025.pdf

⁴⁵ <https://icas.global/wp-content/uploads/AI-In-Advertising.pdf>; <https://www.isba.org.uk/system/files/media/documents/2023-10/AI%20Principles%20-%20Oct%202023.pdf>

An important practical point is that the risk does not depend solely on the AI model itself; it may also arise from the brief/prompt, the selection of creative references, the performance history feeding the optimization process, and the constraints imposed by the campaign itself (e.g., conversion goals that lead the system to concentrate delivery on “cheaper” profiles or those ‘more likely to convert”).

In addition, the use of AI may create an “illusion of neutrality”. Convincing outputs may appear objective and ‘data-driven,’ when in fact they reflect historical patterns and embedded assumptions.

To avoid this effect, it is recommended to adopt a minimum standard of diligence: a checklist addressing stereotypes and sensitive language, human review (with diversity of perspectives whenever possible), controlled testing, and documentation of mitigation decisions (e.g., prompt adjustments, filters, and targeting criteria). This improves the quality of marketing content and reduces regulatory and reputational risks associated with discriminatory practices.

4.5 Security, integrity, and reliability

Security in AI applied to marketing involves protecting inputs (briefs, prompts, data, images, creative assets, and strategic information), preventing leaks and misuse, reducing manipulation risks (including by third parties), and ensuring that the solution operates reliably within its intended context. In marketing, a technical failure quickly becomes a consumer experience failure and a reputational risk; an incorrect output, an inappropriate chatbot response, or manipulated content can generate complaints, regulatory sanctions, legal action, and loss of trust.

Sectoral guidelines and best practices emphasize the need for due diligence in selecting and contracting tools, defining access controls, governance of logs (including what is stored and for how long), and clear incident response and escalation protocols.

Beyond classic security risks, AI introduces specific information integrity risks: outputs may be factually incorrect (including due to “hallucination”), may mix sources, and may sound convincing even when wrong — which requires verification before publishing or responding directly to consumers⁴⁶.

In practice, “reliability” should be treated as a bundle of integrated controls: (i) use of approved tools with appropriate commercial-use terms; (ii) operational security (access roles, environment segregation, protection of data and creative assets); (iii) risk-proportionate human validation (especially for claims, data, comparisons, recommendations, and customer service); and (iv) minimum traceability of what was generated and approved (tool, version, responsible party, and review evidence), enabling auditability and rapid correction when needed.

⁴⁶ <https://icas.global/wp-content/uploads/AI-In-Advertising.pdf>; https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20&%20challenges%20in%20generative%20AI.pdf

4.6. Responsibility and accountability

Accountability in advertising translates into the definition of clear roles between Advertiser, Agency, and Providers regarding who is responsible for the use of AI and for content approval, as well as the preservation of evidence (which tool/model was used, who approved it, which version was published, and which controls were applied).

The Interactive Advertising Bureau (IAB), when addressing disclosure and transparency, reinforces that decisions on labeling and communication cannot be improvised; they require criteria, consistency, and record-keeping⁴⁷. Regulators have also signaled that claims about AI and promises made to consumers require substantiation and do not benefit from a “technology exception”⁴⁸.

4.7. Legality and regulatory compliance

The use of AI in marketing does not occur in a legal vacuum. The Brazilian legal framework already addresses, in a cross-cutting manner, the main risks associated with automation, personalization, content generation, and intensive data use. In practice, this means that the use of AI must comply, cumulatively and in an integrated manner, with: the Consumer Protection Code (CDC); the General Data Protection Law (LGPD); the Brazilian Advertising Self-Regulation Code (CONAR); intellectual property rules, including copyright over content used as input or generated by AI; personality rights, including image and voice rights; as well as the terms of use and policies of platforms and technology tools.

Consumer protection law and rules against misleading/ abusive advertising	Commercial communication remains subject to standards of non-deceptiveness, clarity of information, non-abusiveness, and non-misleading practices, including when content is generated or optimized by AI. This covers (a) product/service claims, (b) comparisons, (c) performance promises, and (d) messages that may exploit vulnerabilities (especially in sensitive topics). Authorities have also signaled enforcement and sanctions against misleading AI-related claims (AI washing) and practices that may induce undue consumer trust through conversational interfaces ⁴⁹ .
Personal data protection (LGPD) in the use of AI	When AI involves personal data (targeting, personalization, profiling, measurement, research based on interactions, or the use of proprietary datasets), the principles and obligations of the LGPD fully apply (purpose limitation, adequacy, necessity/ data minimization, transparency, security, prevention, and accountability). In practice, the critical points typically include: (a) defining legal bases and purposes, (b) data minimization and dataset governance, (c) management of processors and sub-processors (tools and vendors), (d) retention and use of logs, and (e) security measures and incident response. Operational implication: whenever personal data is involved in the workflow, it is recommended to require vendor clarity regarding retention, training use, processing location, and security controls, as well as to document decisions and measures adopted.

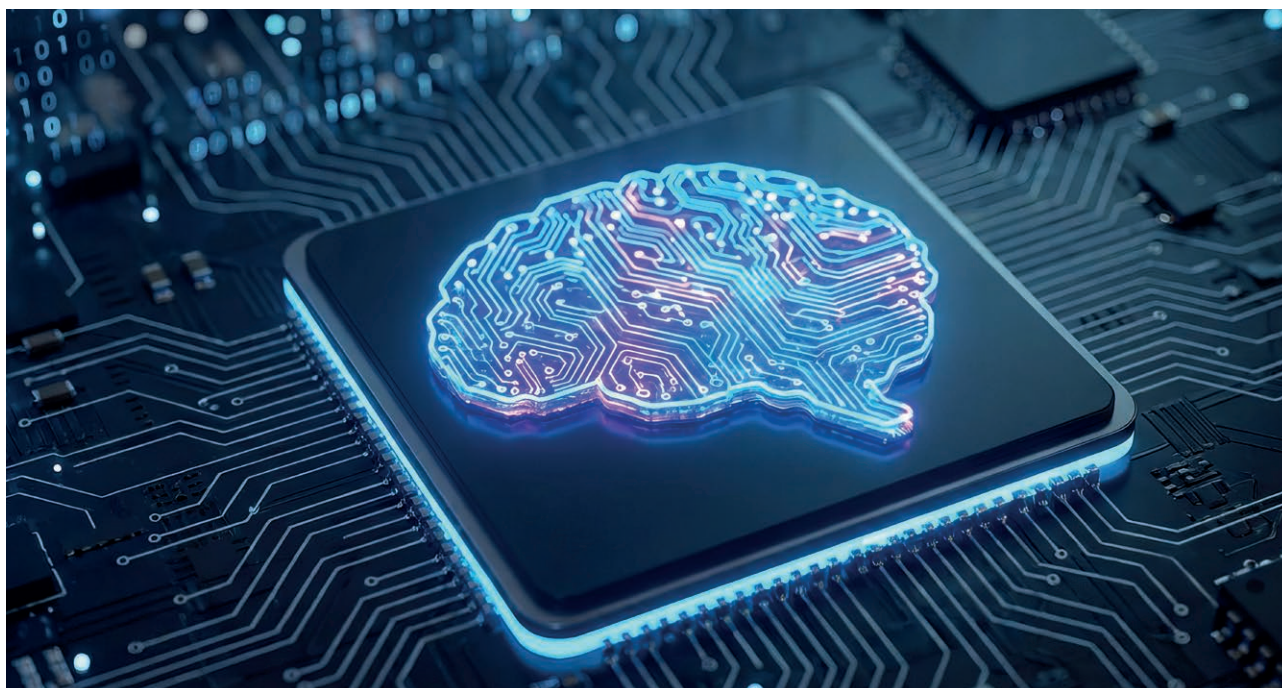
47 <https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/>
48 <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>
49 <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>; <https://eacnry.com/news/chapternews/ftc-chatbots-deepfakes-and-voice-clones-ai-deception-for-sale/>

Intellectual property (copyright, trademarks, licenses, and trade secrets)	In contexts of generative AI, IP risks arise on two fronts: (1) inputs — third-party materials included in the prompt (texts, images, videos, layouts, works, datasets, slogans) (2) outputs — AI-generated assets that may reproduce protected elements, create substantial similarity with existing works, or incorporate third-party trademarks/elements without authorization. Contractual and licensing limitations of tools must also be considered (what is permitted to generate and how it may be used commercially)⁵⁰ Operational implication: to reduce exposure, it is advisable to establish “clearance rules” (review checks) for AI-generated creatives and maintain minimum traceability (tool/version/file) to demonstrate due diligence.
Personality rights (image, voice, name, and identity)	The use of AI can intensify risks related to image, voice, and identity, especially with avatars, voice cloning, realistic manipulation, and deepfakes. Even in lawful campaigns, the use of identifiable likeness (or elements that suggest endorsement) requires heightened care regarding authorization, purpose limitation, usage boundaries, and the prevention of public confusion about authenticity. This issue is particularly sensitive in relation to influencers, celebrities, and “personas” that imitate real individuals. Operational implication: where there is a risk of material confusion, compliance involves not only authorization/clearance but also appropriate transparency and labeling decisions in the creative asset or user experience.
Advertising rules and self-regulation	Beyond the CDC, advertising compliance is also governed by self-regulation, notably CONAR in Brazil and the ICC Code internationally, both grounded in principles such as truthfulness, identifiability, social responsibility, and fairness in communication⁵¹. The presence of AI in the process should be treated as part of the “how” advertising is produced—without changing the “what” is required in terms of honesty and non-deceptiveness.
Terms of use and policies of platforms and tools	In AI-driven campaigns, compliance includes observing (and documenting) what platforms and tools allow in relation to: prohibited categories, data usage, synthetic content, labeling, political advertising, targeting restrictions, and integrity rules (e.g., deepfakes and misinformation). Even when there is no illegality, violations of platform policies may result in ad removal, account suspension, loss of reach, or reputational damage. Operational implication: internal processes and agency/vendor contracts should include obligations to comply with platform policies, maintain evidence, and promptly implement corrections when flags or removals occur.
Emerging regulations and international operations	For groups with international operations (or those working with global vendors), it is relevant to consider foreign regulations that may have practical effects on suppliers and workflows—such as the EU AI Act⁵². And other regimes addressing transparency, synthetic content, deepfakes, and labeling, such as those in China and California. These references should be assessed based on the concrete applicability of each rule and may serve as indicators of regulatory trends, without automatic transposition to operations not subject to such regimes. Therefore, they should not be interpreted, on their own, as equivalent legal obligations in Brazil.

⁵⁰ <https://www.isba.org.uk/system/files/media/documents/2023-10/AI%20Principles%20-%20Oct%202023.pdf>

⁵¹ <https://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf>; https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

⁵² <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>



4.8. Proportionality between risk, control, and impact

The principle of proportionality guides that governance and accountability obligations in the use of AI in marketing should be applied in proportion to risk and impact, taking into account (i) the degree of control the advertiser/agency has over the technology and the outcome, (ii) the predictability of the system (how stable and explainable its behavior and outputs are), and (iii) the potential impact on individuals and consumers.

Risk / impact level	
Low	Internal use for brainstorming, summarization, and drafting support (no direct publication). Typical controls: approved tools, usage guidelines, human review before any publication.
Medium	Generation of creative content variations to be reviewed and approved; media optimization with guardrails. Typical controls: claims/IP checklist, human review, minimum documentation (tool/version), performance monitoring, and brand safety controls.
High	Deepfakes/voice/image realism, public-facing avatars and chatbots, high personalization, campaigns targeting children/vulnerable groups, and automated decisions with discrimination risk. Typical controls: reinforced multi-stakeholder approval, disclosure criteria, controlled testing, enhanced traceability, incident response plan, and rapid escalation mechanisms.

Proportionality thus allows innovation and due diligence to be aligned: the higher the risk and impact, the stronger the required layers of review, documentation, and safeguards.

QUICK CHECKLIST BY PRINCIPLE: QUESTIONS AND EVIDENCE

Principle	Practical decision question	Minimum evidence (to demonstrate compliance)
Legitimate purpose and business alignment	What are we using AI for here, and what outcome do we expect?	Documented objective; scope of use + limitations and approvals
Transparency and explainability appropriate to the context	Could the audience be misled if they are not aware that AI or automation is involved?	Disclosure criteria; label/notice/FAQ; decision log
Human centrality, supervision, and review	What requires human review before going live (and in which cases should it be escalated)?	Review/approval workflow; sampling/monitoring; review records
Non-discrimination, fairness, and bias mitigation	Is there any risk of stereotypes, unfair exclusions, or discriminatory targeting?	Bias testing/checks + sensitivity checklist; review with diverse team
Security, integrity, and reliability	Are we protecting inputs and outputs and preventing misuse?	Access controls; logs; rules for data/prompts; incident response plan
Responsibility and accountability	Who is responsible for outputs, corrections, and incidents?	RACI matrix (roles); contractual clauses and SLAs; rapid response channel
Legal and regulatory compliance	Does it comply with LGPD, CDC/CONAR, and applicable IP/personality rights?	Legal validation when necessary; claims verification; compliance with terms of use
Principle of proportionality between risk, control, and impact	Is the level of control, validation, and human supervision proportional to the risk and potential impact of AI use?	Risk/criticality classification matrix for the use case; record of controls applied consistent with the risk level

5. Key risks and practical safeguards

AI enables scale, automation, and creativity, but also increases the likelihood of error and harm, especially when outputs are published, when there is personalization/targeting, when real people are simulated (image/voice), or when campaigns involve sensitive topics (health, finance, children).

For this reason, this Good Practice Guide establishes safeguards proportional to risk, combining human review, traceability, transparency, data governance, contractual controls, and rapid incident response⁵³.

⁵³ https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

Level	When it tends to occur	Examples	Minimum safeguards
Low	AI as internal support, without personalization and without sensitive claims	Headline brainstorming; insight summarization	Human review; factual checking; basic logging (prompt/version/approval)
Medium	AI generates content that goes public or adjusts creatives/media	Image/copy variations; creative optimization	Enhanced human review; compliance checklist; rights/copyright verification
High	It may confuse/mislead, affect vulnerable audiences, use data/biometrics, or simulate real people	Deepfakes/synthetic voice; “human” avatars; offer-driven chatbots; sensitive audience segmentation	Legal/compliance approval; public transparency; testing/validation; full traceability; incident response plan

5.1. Deceptive or abusive advertising; AI washing and claims about AI

AI washing is the practice of exaggerating, distorting, or vaguely presenting AI capabilities in order to make a product or service appear more attractive, or to attribute undue authority to the use of AI to increase credibility or justify price/performance, without real supporting evidence⁵⁴.

In general, it appears in three forms:

1. AI as a generic label (mentioning AI without minimally explaining what it does)
2. absolute claims (“100%”, “error-free”, “infallible”, “guaranteed”)
3. misattributed trust (using AI to simulate neutrality, auditing, certification, or expertise)

This type of practice is increasingly scrutinized by authorities, including initiatives aimed at combating misleading claims and AI-related schemes⁵⁵. In practice, it is important to keep in mind that saying “we use AI” or “AI did it” does not reduce responsibility and does not replace evidence. On the contrary, it may raise the expected standard of due diligence, as it creates a perception of technological superiority⁵⁶.

Practical safeguards

1. **Substantiation rule for claims:** every AI-related claim (accuracy, efficiency, safety, performance) must be supported by verifiable evidence kept for audit purposes
2. **Governance of AI claims:** AI claims must be validated jointly (Marketing + Product/IT + Legal/Compliance)
3. **Communication with clear limits and precise language:** prefer concrete descriptions (“uses AI to suggest...”, “assists...”) and avoid absolute superlatives (“perfect”, “guaranteed”)
4. **Evidence archiving and traceability:** store final versions, justifications, tests, and approvals

⁵⁴ <https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html>; https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust/; <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>

⁵⁵ <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>; <https://eaccny.com/news/chapternews/ftc-chatbots-deepfakes-and-voice-clones-ai-deception-for-sale/>

⁵⁶ https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust/



WHAT TO DO	WHAT NOT TO DO
✓ Describe AI in a concrete and verifiable way (what it does, what it is for, and its limitations) ✓ Validate “sensitive” claims (accuracy, safety, impacts) before going live ✓ Replace generic “AI” wording with functional descriptions (“automates screening”, “generates variations”, “optimizes bids”) and use language proportional to what can actually be demonstrated ✓ Maintain substantiation and evidence for relevant claims (tests, metrics, limitations, and conditions) ✓ Carefully review AI-generated pieces and scripts, especially for facts, numbers, comparisons, and promises ✓ In conversational experiences, design flows to reduce “overconfidence”: safe responses, clear limits, human escalation, and proportionate transparency	✗ Do not attribute automatic authority to AI ✗ Do not promise accuracy or guaranteed results without robust evidence ✗ Do not use AI as a “badge” of superiority without strong evidence and appropriate context ✗ Do not make absolute claims (“100%”, “infallible”, “error-free”) or present results as guaranteed by AI ✗ Do not use testimonials, reviews, or social proof or synthetic demonstrations in a way that could be perceived as real by consumers ✗ Do not assume that disclosure eliminates risk: transparency does not replace compliance with consumer protection rules or self-regulation, nor does it “shield” against claims of misleading or abusive practices

5.2. Synthetic Content and Integrity

Synthetic content is any material (text, image, audio, video) generated or altered by AI. The key point is not its synthetic nature, but the impact it may have on the integrity of communication.

Examples include: simulation of real people (deepfakes), creation of testimonials that appear authentic, alteration of visual evidence (“before and after”), or manipulation of context in a way that leads consumers to believe something that did not actually occur.

In marketing, this is especially critical because trust is an asset, and highly realistic content can reduce the audience’s ability to distinguish fiction from reality⁵⁷.

⁵⁷ https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

Practical safeguards

- 1. Proportionate transparency based on risk:** if the absence of information may lead to misunderstanding, recommend disclosure (“AI-generated image”, “synthetic voice”, etc.)
- 2. Authorizations and controls for image/voice use:** use of image/voice/avatars requires formal authorization and clearly defined scope
- 3. Origin and creation traceability controls:** maintain logs, versions, and records of the generation process
- 4. Rapid response:** establish procedures for removal/rectification in cases of public confusion or material error

WHAT TO DO	WHAT NOT TO DO
✓ Treat “synthetic content” as a mandatory item in the pre-publication checklist (“could this be misleading?”→“does it require disclosure?”) ✓ Strengthen human review when there is simulation of people, “social proof,” or testimonials	✗ Do not create fake testimonials, synthetic reviews, or artificial social proof ✗ Do not simulate a real person without authorization (including image, voice, or recognizable mannerisms)

Therefore...

the disclosure that content was generated by AI (e.g., watermarks or notices such as “AI-generated image”) should be assessed on a case-by-case basis and is generally recommended when the absence of this information may create a concrete risk of material misunderstanding by the consumer regarding the nature, authenticity, origin, endorsement, or characteristics of the product or service being offered. When the use of AI is merely instrumental (e.g., internal creative support), does not alter facts, does not simulate a real person, does not artificially enhance credibility, and does not influence the weight of the advertising claim, disclosure may not be necessary or may be provided in a simplified and contextual manner, preserving communication flow.

In summary, labeling should be proportional: sufficient to prevent material deception, without turning legitimate use of AI into unnecessary noise in the consumer experience.

5.3 Synthetic personas and synthetic data

Synthetic personas are characters/avatars (including virtual influencers and assistants) created using AI to communicate, interact, “converse,” and generate content. These personas can achieve a high degree of realism and, precisely for that reason, have strong potential for engagement and persuasion.

The risk arises when there is:

- Meaningful confusion regarding the non-human nature of the interaction
- Simulation of experience or authority that does not exist
- Improper exploitation of trust or vulnerability

The central regulatory criterion is not the existence of a virtual persona itself, but the potential to induce material misunderstanding.

Synthetic personas are legally viable and strategically valuable, provided that the interaction maintains sufficient clarity about their nature when this is relevant to audience understanding.

Practical safeguards

- 1. Transparency in interaction:** make it clear when the user is interacting with a persona/virtual assistant, but only when there is a risk of confusion
- 2. Limits on persuasion:** prohibit scripts and strategies that exploit emotional vulnerabilities, especially with children
- 3. Synthetic data governance:** document purpose, methodology, risk testing (re-identification/inference), and biases. If synthetic data generation uses personal data as input, the activity remains subject to data protection law (purpose limitation, adequacy, necessity, security, prevention, and accountability). “Becoming synthetic” does not remove governance obligations over the source data, nor does it allow unrestricted reuse
- 4. Contracts and rights:** define ownership/licensing of the avatar/persona, scope of use, termination, and removal



WHAT TO DO	WHAT NOT TO DO
✓ Use synthetic personas as clearly identified characters with a defined “limits script” (what they can and cannot say) ✓ Document the use of synthetic data (origin, method, purpose, and tests): what data was used, why it was generated, and where the synthetic data can (or cannot) be applied ✓ Apply privacy and security controls in generation: minimization, anonymization where applicable, retention and access rules, and re-identification risk assessment ✓ Perform bias and stereotype checks on personas and outputs, with human review and evaluator diversity ✓ If used externally (reports, disclosures, content), clearly describe methodology and limitations, avoiding confusion between simulation and real research findings	✗ Do not present synthetic personas as “real consumers” or as a completed “market research study”; this may mislead and increase reputational and regulatory risk ✗ Do not allow the persona to “improvise” sensitive offers without human supervision (especially in chatbots) ✗ Do not use synthetic data generated from personal data without clear governance (purpose, retention, security, vendors) ✗ Do not use synthetic personas to justify sensitive segmentation, exclusions, or high-impact decisions without additional validation and non-discrimination controls ✗ Do not treat “convincing” outputs as “true”: simulations may reflect model and prompt bias

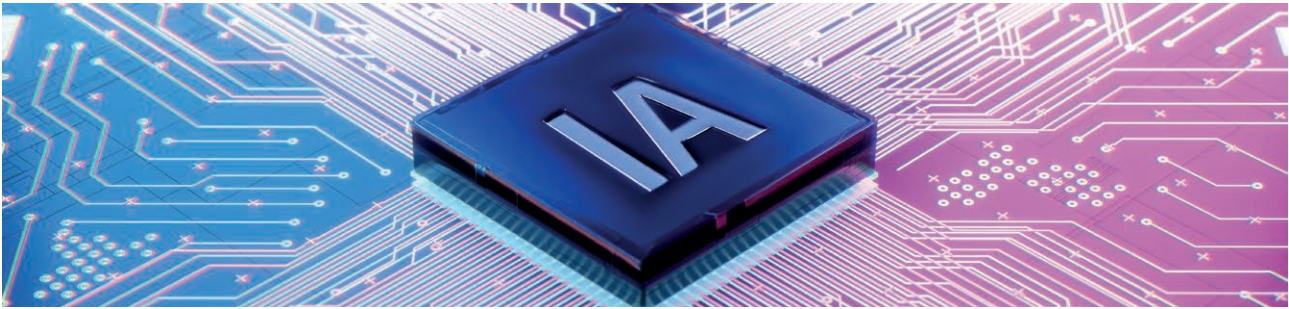
5.4 Bias, Discrimination, and Stereotypes

Bias in AI occurs when models reproduce distorted patterns from training data or usage context, which can lead to discrimination (unfair treatment) or stereotypes (reductive representations of groups).

In marketing, the risk appears both in content (images/texts that reinforce prejudice) and in operations (segmentation and optimization that exclude audiences or exploit vulnerabilities). Since platforms and tools “learn” from historical data, they may reproduce societal inequalities and problematic preferences without this being visible in the final output.

Practical safeguards

- 1. Human oversight** focused on data governance, diversity, equity, and inclusion
- 2. Testing and sampling** of inputs, outputs, and segmentations to detect discrimination
- 3. Clear guidelines for language and casting** (red lines against stereotypes and sensitive attributes)
- 4. Continuous monitoring** (bias is not a one-time event: it may emerge due to changes in data, trends, and context)
- 5. When AI-driven content generation, selection, or operational control** is handled by an agency or vendor, contractual obligations should require independent and proportionate review to mitigate bias, including documentation of checks performed and escalation to the advertiser when relevant risk is identified



WHAT TO DO	WHAT NOT TO DO
✓ Incorporate equity and inclusion as a quality requirement: treat bias as a brand and compliance risk, not a secondary issue ✓ Review AI inputs and outputs using a stereotype/representation checklist and, where relevant, diverse evaluators ✓ When content generation or selection is handled by an agency/vendor, contractually require them to perform or enable this review, while maintaining evidence for advertiser validation ✓ Monitor targeting and delivery to identify unintended exclusions and adjust parameters and creatives accordingly ✓ Document mitigation and correction decisions (prompts, filters, libraries, adjustments)	✗ Do not assume automatic neutrality — convincing outputs may carry biases from the model and context ✗ Do not automate segmentation/ optimization without guardrails and review when there is potential for unequal impact ✗ Do not publish content that reinforces stereotypes (gender, race, age, disability, class, territory), even if “unintentional”: the criterion is the effect and how it is likely perceived by the audience

5.5 Intellectual Property and Personality Rights

Generative AI has expanded the ability to create text, images, videos, soundtracks, voiceovers, and avatars at scale, but this does not remove legal obligations regarding intellectual property (IP) and personality rights. On the contrary, as production becomes faster and more distributed, the risk increases that protected content may be used without a license, that “similarities” with existing works or real individuals go unnoticed, and that contractual rules (platform terms, stock libraries, voice/image banks, agency and talent agreements) may be breached.

In campaigns, the most common issues arise in three areas: (i) inputs (what is fed into the tool — briefs, prompts, images, references, assets, and data), (ii) outputs (what the tool generates — and whether there is a risk of substantial reproduction, similarity, trademarks/works/characters, or recognizable “voice/image”), and (iii) use and licensing (how the output will be exploited — commercially, across which media/territories, and under which terms, including retention, reuse, and potential training by the provider).

Practical safeguards

- 1. Rights checklist before publishing:** verify licenses, releases, authorizations, stock media terms, and compatibility with intended use (media, territory, duration), as well as similarity/confusability risk checks
- 2. Agency/vendor contracts:** include rules on third-party inputs; obligation to disclose internal AI usage; representations and warranties that the agency/vendor holds necessary rights for all materials used and that inputs and outputs do not infringe third-party rights; indemnification obligations in case of claims; limits on reuse/exclusivity; and an obligation to maintain evidence of clearance and documentation of origin/licenses where applicable and proportionate to risk
- 3. Training and reuse of advertiser materials:** prohibit training, fine-tuning, or reuse of advertiser materials to improve vendor models without explicit authorization, with clearly defined scope, purpose, retention, security, and auditability
- 4. Internal confidentiality and “allowed inputs” policy:** define what can/cannot be entered into tools (including unreleased assets, strategy, trade secrets, personal data, and licensed materials with restrictions), and train teams and partners accordingly

WHAT TO DO	WHAT NOT TO DO
✔ Treat any AI tool as a vendor: validate terms, commercial use rights, retention, and reuse before adoption ✔ Require the vendor to provide documentation of origin/licenses where applicable and proportionate to risk; define ownership of the final deliverable and include contractual representations, warranties, and indemnification for violations of intellectual property rights, personality rights, and any other third-party rights ✔ Adjust contracts to prevent “default training” using advertiser materials ✔ Include specific contractual clauses: AI disclosure, source of inputs, rights over outputs, reuse, indemnification, audit rights, and subcontractors ✔ Define and enforce a “permitted inputs” rule (what can be entered into prompts) + train internal teams and agencies ✔ Conduct prior clearance: IP and personality rights checks focused on similarity/confusability and presence of recognizable trademarks, works, or personas	✘ Do not assume that “the output is automatically original” or that “if AI generated it, it is cleared for use” ✘ Do not ask AI to “imitate” a work/artist/brand in a way that creates unauthorized derivative content ✘ Do not use a real person’s voice/image (or highly similar likeness) without authorization ✘ Do not use voices/images that are “very similar” to celebrities, influencers, or real individuals without authorization (even if not identical) ✘ Do not use “free” or non-approved tools for sensitive projects, or input assets, confidential briefs, or business data into them ✘ Do not feed third-party materials into AI (images, music, scripts, slogans, characters) without a license or outside the scope of the license

WHAT TO DO	WHAT NOT TO DO
✓ Ensure explicit authorizations for the use of image/voice/name/likeness when involving real individuals or any risk of recognizability ✓ For avatars and characters, assess the risk of material confusion and apply proportionate disclosure when necessary ✓ Establish a rapid response process: if there is any IP/personality rights challenge, pause the campaign and review assets and approvals	✗ Do not accept “generic” contracts that do not define responsibility for inputs/outputs and for intellectual property/personality rights violations ✗ Do not ignore risk signals (similarity complaints, takedown requests, reports); delays in taking response measures increase harm and exposure

5.6. Personal Data in Model Training

When it comes to training AI models, special care is required to ensure compliance with privacy and data protection laws. Among the various elements addressed in the data protection section of this guide, two deserve particular attention in the context of AI training: transparency and the legal basis for processing personal data in the training of AI models.

Transparency: effective communication with data subjects is necessary so that they can meaningfully understand how their data is used in the training of AI models and for what purpose.

Practical safeguards

How to ensure adequate transparency?

In addition to the requirements outlined above (as per item 3 of this guide), the following additional measures are recommended in the context of AI training⁵⁸:

- ✓ Actively inform data subjects, whenever possible, about the use of their data for this purpose
- ✓ Provide individuals with information such as the categories of data used, their origin, and how to exercise their rights, especially the right to object
- ✓ Make such information available at the time of initial data collection or, when this is not possible, at the first subsequent contact with the data subject

LEGAL BASIS

As a general rule, provided there is no processing of sensitive personal data, such processing may be based on legitimate interest, provided that the balancing test requirements are met (as per item 4.2 of this guide). There are additional recommendations to those already presented throughout this guide that may help support the proper use of this legal basis:

⁵⁸ <https://www.cnil.fr/fr/node/165891>

Situation	Recommendations
Personal data collection ⁵⁹	✓ Define in advance which personal data you need to process and for what purpose ✓ Perform data filtering prior to collection, using precise criteria to reduce the risk of accidental collection of sensitive personal data, data from children and adolescents, or irrelevant data ✓ Perform data filtering after collection, but before training the AI model ✓ Document data filtering processes ✓ When collecting data from public sources, respect websites that clearly object to scraping (e.g., via robots.txt). In addition, remove excessive datas⁶⁰
Exercise of data subject right	✓ Ensure that data subjects can object to the use of their personal data for AI model training ✓ Ensure that the right to object is made available in a simple and intuitive way, ideally prominently within privacy settings or another solution adopted by the organization for receiving and handling data subject requests⁶¹
Transparency	✓ If data subjects do not have a prior relationship with the organization (and therefore have not had the opportunity to access the Privacy Notice), proactively notify them whenever possible ✓ Follow the transparency recommendations outlined in the table above
Data minimization ⁶²	✓ Anonymize data immediately after collection ✓ Assess the feasibility of using synthetic data (e.g., artificially created data designed to statistically resemble real data, without referring to real individuals or real events)

OBSERVATIONS:

- Compliance with these recommendations does not necessarily ensure that the processing is adequately framed. Each specific case must always be assessed individually
- Framing model training under legitimate interest does not necessarily mean that the use of the model relies on the same legal basis; it is possible, for example, for training to be based on legitimate interest while the use of the model may require the data subject's consent⁶³

⁵⁹ https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

⁶⁰ <https://www.cnil.fr/en/legal-basis-legitimate-interest-focus-sheet-measures-implement-case-data-collection-web-scraping>

⁶¹ ANPD. ANPD. Vote n° 11/2024/DIR-MW/CD. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf

⁶² <https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system>

⁶³ <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-46-2024.pdf>

WHAT TO DO	WHAT NOT TO DO
✓ Define the purpose and scope of training (objective, data categories, sources, retention period, recipients, and processing environment) ✓ Use only strictly necessary data; prefer aggregated, pseudonymized/ anonymized data where feasible ✓ Perform prior dataset screening/filtering (removal of sensitive data, children/adolescents' data, and irrelevant data) ✓ Document the legal basis and justification for data use in training, including proportionality and risk assessments ✓ Ensure proportionate transparency regarding data use in training where applicable and provide channels for data subject rights requests ✓ Implement and operationalize the right to object where applicable, with defined internal workflows and responsible parties ✓ Establish contractual rules with agencies/vendors: prohibition of reuse/training with advertiser data without explicit authorization; retention, deletion, and audit requirements ✓ Assess lower-risk alternatives (e.g., synthetic data, reduced samples, anonymization techniques) when they achieve the intended objective ✓ Define an internal approval process for projects involving personal data training (privacy/legal/ security gate, based on risk level)	✗ Do not train AI on broad, undefined datasets (“use everything available”) without a specific and documented purpose ✗ Do not mix sensitive data or minors’ data into training without justification, enhanced controls, and applicable authorization ✗ Do not use generic texts that fail to explain purpose and relevant implications ✗ Do not make it difficult or impossible to exercise opt-out/erasure rights by creating friction or lacking an effective channel ✗ Do not allow “default training” by vendors using advertiser data through vague clauses or lack of contractual provision ✗ Do not freely share datasets across multiple teams/third parties without access controls and traceability ✗ Do not use real personal data out of convenience when less intrusive alternatives would suffice ✗ Do not run “pilot” projects with personal data without prior validation and minimum governance and security controls

5.7. Information Security in AI

When addressing information security in the context of AI, three recurring risks must be considered: (a) traditional cyberattacks, which could affect any AI system; (b) AI-specific attacks, known as adversarial attacks; and (c) human errors in the use of AI, which may expose personal data and the organization’s confidential information.

For traditional cyberattacks and AI-specific attacks, responsibility generally lies with those in charge of developing and implementing AI solutions. Therefore, depending on the organization’s role, these guidelines may serve both as a benchmark for fulfilling its own responsibilities and as a

reference for defining contractual requirements for vendors. In relation to human errors in the use of AI, the guidelines are specifically intended for users of AI solutions.

a) Traditional cyberattacks

AI systems, like any other systems, rely on informational and computational assets to function—such as databases, processing infrastructure, applications, APIs, among others. These assets are subject to ordinary information security risks⁶⁴ and must be integrated into the organization's existing information security management system and protected with appropriate technical measures, such as access controls, encryption, vulnerability management, encrypted backups, logging, data leakage prevention practices, and others.

It is also worth noting that if personal data is involved in the context of an attack and there is a relevant risk or harm to data subjects, it is recommended to assess the applicability of ANPD Resolution CD/ANPD No. 15—Security Incident Communication Regulation, including any obligation to notify the ANPD and data subjects, the adoption of appropriate technical, administrative, and governance measures, as well as proper documentation and structured analysis of the incident.

b) AI-specific attacks

Mode	Description ^{64,65}
Abuse	Attacks in the data collection phase, involving the introduction of inappropriate information into legitimate sources, inserting incorrect information that the system absorbs, with the aim of diverting or distorting the intended use of the model, without directly altering the formal training process.
Poisoning	Attacks in the training phase that introduce corrupted or biased data into the training dataset, causing the model to learn inappropriate patterns.
Evasion	Attacks in the testing or operational use phase of the AI system, in which the attacker minimally manipulates inputs provided to the model, without altering its training or internal parameters, with the aim of inducing incorrect classifications or decisions during inference (e.g., providing an autonomous vehicle system with stop signs that have small alterations so that it misclassifies stop signs as speed limit signs).
Privacy	Attacks during the operational use phase in which attackers seek to infer sensitive information about the model or its training data through legitimate interactions used for reverse engineering, source exploitation, or identification of vulnerabilities.

⁶⁴ <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

⁶⁵ <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

⁶⁶ <https://csrc.nist.gov/pubs/ai/100/2/e2025/final>



Practical safeguards⁶⁷

1. **Adversarial training:** mitigation techniques that train the model with intentionally perturbed examples, aiming to increase its resistance to attacks during inference
2. **Randomized smoothing:** techniques that add controlled noise to inputs to make model predictions more stable against small adversarial perturbations
3. **Data sanitization:** techniques designed to clean the training dataset and remove poisoned samples before training the machine learning model
4. **Model inspection and sanitization:** techniques for evaluating the model before deployment to detect and correct signs of poisoning or abuse

NOTE

The controls to be implemented will always depend on the specific case. However, the attacks described above and the illustrative measures may be used as a reference when assessing risks involving the development or implementation of an AI model, especially when made available to the general public (e.g., chatbots).

c) Human errors in the use of AI

When employees use AI solutions in their daily work (especially generative tools and conversational assistants), information security depends less solely on the technical robustness of the provider and more on the operational behavior of the users. Prompts, attachments, and interactions may inadvertently expose personal data, confidential information, and creative assets; in addition, certain configurations may increase the risk of improper reuse of the content entered into the system.

Therefore, even “trusted” tools can become a source of incidents if they are used without clear rules on access, configuration, and permitted content, making internal policies, training, and specific safeguards for employee use essential.

⁶⁷ <https://csrc.nist.gov/pubs/ai/100/2/e2025/final>

Practical Safeguards

- 1. Contractual guarantees and retention policy:** obtain assurances from the vendor regarding data retention, reuse, and training with company data (opt-out by default whenever possible), as well as regarding subprocessors and data transfers
- 2. Golden rule for inputs:** prohibit the insertion of confidential information (strategy, contracts, pricing, media plans, negotiations, client lists) and personal data, except in approved tools and authorized use cases
- 3. Input classification rule:** create a simple classification matrix (“allowed”, “allowed with caution”, “not allowed”) for prompts and attachments, including NDA-protected materials, unreleased creative assets, and internal documents
- 4. Approved tools and shadow AI blocking:** allow only approved corporate tools and discourage the use of personal accounts or unauthorized plugins for work purposes
- 5. Access control and permission segregation:** apply the principle of least privilege (who can use which tools and with what capabilities), with SSO (Single Sign-On), MFA (Multi-Factor Authentication), and rapid access revocation upon offboarding
- 6. Logs, monitoring, and minimal auditing:** maintain access and usage logs (where possible and proportionate) for incident investigation and policy improvement, with controlled retention and access
- 7. Ongoing training and communication:** provide short, recurring training with real-life examples (what is sensitive data, what should not be included in prompts, how to configure privacy settings, how to report incidents)
- 8. Incident playbook:** create a simple procedure for “I used AI and may have exposed something” — who to notify, how to record the incident, how to contain it (revoke links, pause integrations, notify IT/Legal/Privacy teams)

WHAT TO DO	WHAT NOT TO DO
✓ Approve tools based on minimum security criteria, terms of use, data retention policies, training with data, and support for logging and incident response ✓ Define an “allowed inputs” policy: what can and cannot be entered (personal data, trade secrets, strategies, contracts, unreleased assets, third-party materials) ✓ Disable the use of prompts/files for model training whenever possible; restrict history and sharing features	✗ Do not treat security as an exclusive IT responsibility, without operational rules for the marketing team and external partners ✗ Do not allow the use of unapproved tools, personal accounts, or unvalidated extensions/plugins ✗ Do not share credentials or access, nor maintain overly broad permissions simply to “facilitate operations”

WHAT TO DO	WHAT NOT TO DO
✓ Maintain logs and traceability proportional to risk (access, usage, versions, integrations, relevant changes), with defined retention and access controls ✓ Establish an incident response playbook: how to contain (pause bot/campaign), preserve evidence, escalate to responsible stakeholders, and communicate internally ✓ Provide periodic training for employees with practical examples (what must not be entered, how to configure systems, how to report incidents)	✗ Do not connect AI to internal systems (CRM, databases, drives) without safeguards against prompt injection and without clearly defined access scope boundaries ✗ Do not engage or use vendors without minimum security commitments, leaving security obligations undefined or unclear

5.8. Children and vulnerable groups: enhanced safeguards (content, targeting, persuasion)

The use of AI in marketing can increase the ability to personalize messages, dynamically adjust advertising materials in real time, and conduct conversational interactions with a high degree of persuasive power. When the audience includes children/adolescents or vulnerable groups (due to socioeconomic condition, age, health status, indebtedness, emotional fragility, low digital literacy, etc.), these mechanisms raise the risk of undue manipulation and violation of responsible advertising standards. Therefore, an enhanced level of due diligence is recommended. It is not enough to simply “comply with general rules”; campaigns must be designed with specific guardrails for protection, transparency, and appropriateness⁶⁸.

Where AI increases risk (and why):

- **Optimized persuasion and continuous testing:** optimization systems quickly learn which messages generate more clicks, engagement, and conversions. In vulnerable audiences, this may lead to the delivery of more aggressive sales-oriented content (e.g., artificial urgency, guilt, fear, insistence), with a greater impact than on fully informed adults
- **Conversational interactions (chatbots, avatars, “virtual friends”):** humanized interfaces can create disproportionate trust, especially in children, who tend to interpret such interactions as real social relationships. The boundary between information, entertainment, and persuasion may become less clear
- **Targeting and sensitive inferences:** AI can infer preferences, emotional states, and propensity toward certain behaviors. In vulnerable groups, this may approach undue persuasion, particularly when combined with timing and highly personalized micro-context targeting

⁶⁸ https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; <https://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf>; <https://icas.global/wp-content/uploads/AI-In-Advertising.pdf>

Practical safeguards

1. **Lower-tolerance risk policy:** campaigns involving children/vulnerable groups must follow stricter criteria for personalization, conversational formats, and automated optimization
2. **Content guardrails:** prohibit pressure-based language (e.g., “if you don’t buy...”, “last chance”), inappropriate emotional triggers, and messages that exploit fear or guilt, especially in sensitive contexts
3. **Targeting controls:** review targeting criteria, avoid sensitive inferences, and restrict lookalike modeling/expansion when audiences include minors or vulnerable groups
4. **Service design for interactions:** in chatbots/agents, use age-appropriate language, avoid simulating emotional or affective relationships, limit recommendations, and escalate to a human when vulnerability signals are detected
5. **Enhanced human review:** require dual review (creative + compliance) for campaigns and user journeys with elevated risk exposure

WHAT TO DO	WHAT NOT TO DO
✓ Treat children/vulnerable groups as a high-risk category for AI use (personalization, chatbots, optimization) ✓ Restrict automation and require enhanced human review for sensitive messages and user journeys ✓ Ensure appropriate transparency in conversational interactions and avoid creating “social confusion” (e.g., appearing as a friend or therapist) ✓ Document decisions: why the targeting/segmentation was chosen, and which limits and controls were applied	✗ Do not use AI to exploit impulsiveness, fear, guilt, or artificial urgency, especially with minors ✗ Do not use chatbots/avatars to simulate counseling or emotional relationships, nor to pressure decision-making ✗ Do not apply lookalikes /expansion without safeguards when there is a risk of inadvertently reaching minors or vulnerable individuals

5.9. Sustainability and social impacts (energy, supply chain, reputation)

The use of AI in marketing also brings impacts that go beyond the campaign itself: energy consumption, dependence on third-party infrastructure, supplier choices, and social effects associated with large-scale automation.

Although many organizations treat sustainability as a “corporate-level” topic, AI makes it operational: decisions about tools, generation volume, automation levels, and vendor governance can affect environmental footprint, reputational risk, and stakeholder expectations.

a) Energy and efficiency (what changes with AI)

Generative models may require significant computational resources, especially in intensive applications (video, high-resolution image, mass generation, training, and fine-tuning). It is important to assess: proportionality of use, reuse of assets, and waste-reduction strategies (e.g., avoiding the generation of hundreds of variations without necessity)

b) Supply chain (risks and due diligence)

AI in marketing often involves multiple vendors: models, platforms, plugins, image/voice databases, and annotation services. This expands risks related to:

- **opacity** regarding where and how processing takes place
- **dependency** on a single vendor and risks of unavailability or policy changes
- **contractual** and security compliance
- **ESG expectations** across the supply chain

c) Social impacts and reputation

AI can generate negative repercussions when it:

- improperly replaces creative work without internal transparency or creates intellectual property conflicts
- produces stereotyped content or misinformation
- is perceived as “unfair automation” (e.g., synthetic personas “pretending” to be real consumers)

In addition, environmental or responsibility claims (green claims) associated with AI must follow the same substantiation rigor: claiming “sustainable AI” without evidence may increase reputational and regulatory risk.

WHAT TO DO	WHAT NOT TO DO
✓ Include sustainability as a criterion in tool selection and approval (efficiency, governance, and supplier transparency) ✓ Reduce “generation waste”: define volume limits, reuse assets, and standardize prompts/briefs to avoid rework ✓ Assess reputational risks: ensure adequate transparency, integrity, and respect for intellectual property and personality rights ✓ Require minimum governance information from suppliers (security, retention, subprocessors), aligning with supply chain due diligence	✗ Do not encourage mass generation without a clear purpose (“generate for the sake of generating”), especially in heavy formats (image/video) ✗ Do not use sustainability as a marketing narrative (“green AI”, “low impact”) without evidence and clearly defined criteria ✗ Do not outsource without governance: supplier opacity and policy changes can become operational and reputational risks ✗ Do not authorize AI use without minimum mandatory training, especially for roles that publish content or interact with consumers

6. AI Governance Applied to Advertising (How to Implement It)

This section brings together governance practices designed to make the use of AI in marketing operational and practical on a day-to-day basis, with clear approval criteria, traceability, and accountability throughout the entire chain, always following a pragmatic and risk-proportionate approach (see the principles set out in Sections 4 and 5 of this guide). The objective is to reduce legal and reputational risks without hindering creativity, by establishing minimum routines, roles, and evidentiary requirements.

6.1 Transparency with the public: when and how to disclose the use of AI⁶⁹

Transparency does not, as a general rule, imply a mandatory requirement to label or identify the use of AI. Any disclosures regarding the use of AI should be assessed on an exceptional, contextual, and risk-based basis, taking into account the potential for consumer confusion and the current state of the regulatory debate in Brazil.

It is important to note that this topic is still evolving and, therefore, there is no consensus — including within Brazilian advertising self-regulation frameworks and international discussions — regarding a duty to label content generated or supported by AI. Accordingly, the guidelines below should be understood as best-practice parameters for case-by-case risk assessment, rather than as a sector-wide obligation or a presumption of irregularity in the absence of disclosure.

PRACTICAL CRITERION

Considering the context of the advertising campaign, disclosure may be advisable, depending on the specific circumstances, when the use of AI may influence the consumer's decision-making or understanding and: (i) involves a high degree of realism (voice/image/avatars, deepfakes, or synthetic content that appears factual); (ii) creates conversational interactions that appear human; (iii) automates segmentation/optimization decisions with relevant impact; or (iv) affects sensitive audiences (such as children or vulnerable individuals) or sensitive topics (such as health or finance).

Disclosure Trigger	Decision Questions	Typical Example	How to disclose
Human-like interaction	Could the consumer reasonably assume they are interacting with a real person? Is there a risk of misleading promises or representations?	Customer service chat with AI-generated responses	Especially for vulnerable audiences, provide clear notice at the beginning of and throughout the interaction: "AI-powered automated service."
Highly realistic synthetic content	Could the audience mistake it for a real recording or photograph? Could there be a "reasonable surprise" effect?	Image of a model with AI-enhanced hair treatment/effects	Visible label in the advertisement/content description and, where applicable, disclosure in the audio or caption.

⁶⁹ <https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/>

Disclosure Trigger	Decision Questions	Typical Example	How to disclose
Image, voice, name, or likeness of a real person	Could it create the perception of endorsement or authorization?	Voice-over “cloned” to resemble a celebrity	Assess contextually. Disclosure may be necessary where it could create a perception of endorsement or otherwise directly affect the consumer’s purchasing decision or understanding of the message.
Claims regarding the use of AI as a product differentiator	Is the claim verifiable and unlikely to create undue trust or mislead consumers?	“100% created by AI”, “AI guarantees results”	Explain the limits and basis of the claim (lettering and/or qualifiers); provide evidence and internal documentation; avoid exaggeration
Content involving sensitive topics or vulnerable groups	Is there a risk of manipulation, stigmatization, or amplified deception?	Beauty product campaign using AI-generated avatars targeted at teenagers	Provide disclosure and enhanced safeguards; ensure human review and appropriateness of tone.
“Internal” use with no direct consumer exposure	Is there any material element perceptible to the public?	AI used solely for brainstorming and draft preparation	As a rule, no disclosure to the consumer is required; internal records must be maintained.

How to disclose: communication should be clear, use simple language, and appear close to the point of interaction (within the advertisement, at the beginning of the interaction, or in another easily accessible location). Disclosure does not replace compliance obligations (see Sections 4.7 and 5) and should remain aligned with advertising self-regulation principles requiring honest and non-misleading communications.⁷⁰

RECOMMENDED PROCEDURE

- Disclose the use of AI when it is relevant to understanding the advertisement, product/service, or interaction, or when it may directly affect the consumer’s purchasing or usage decision.
- Use simple language and provide disclosure at the point of interaction (within the advertisement, interface, or at the beginning of the conversation).
- Where disclosure is appropriate, specify at which stage AI was used (e.g., “AI-generated image,” “synthetic voice,” or “AI-assisted customer service with human supervision”).
- Maintain internal records documenting the rationale for disclosure (why, where, and in which materials/channels disclosure was provided).
- Assess whether disclosure of AI use is necessary whenever omission could create a concrete risk of material confusion regarding the authenticity, origin, endorsement, or characteristics of the communicated content.
- Avoid indiscriminate labeling of all AI uses (“label fatigue”) and avoid concealing disclosures in ineffective fine print or footnotes.

⁷⁰ https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; <http://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf>

6.2 Assessment for the hiring of agencies

The assessment is a practical due diligence process designed to reduce legal, reputational, ethical, data protection, and Intellectual Property risks before hiring or renewing contracts with agencies that will use AI. It should combine objective questions, documentary evidence, and contractual clauses ensuring human review, traceability, transparency, security, and accountability for outputs.

It is also advisable for the assessment to evaluate, from the early stages of the engagement process, the extent of responsibility assumed by the agency or vendor for AI-generated or AI-assisted inputs and outputs, including in cases involving third-party claims arising from unauthorized use of intellectual property or personality rights. This analysis should consider representations and warranties, indemnification obligations, any limitations of liability, contractual exclusions, and claim-response procedures, allowing the advertiser to calibrate legal risks and commercial expectations before moving forward with negotiations.

MINIMUM QUESTIONS AND EVIDENCE

Topic	Practical Questions	Minimum evidence
Governance and training	Is there a designated AI lead or committee? Is ongoing training provided?	Internal policy; training records; designated responsible person
Tools and subcontracting	Which tools will be used and for what purpose? Has the Advertiser expressly approved the use of these tools? Are there any third parties/subcontractors involved?	List of approved tools, including purpose and version; subcontractors; workflows
Human review and quality control	What levels of human review are applied before publication? Is fact-checking conducted?	Review/approval workflow; checklists; sampling procedures
Transparency	How are notices/disclosures implemented when required?	Disclosure templates; examples; decision logs
Data and confidentiality	How does the agency avoid entering personal or confidential data into prompts?	Rules regarding permitted data; controls; contractual clauses
Intellectual Property and personality rights	How does the agency document the origin/licenses and authorizations, where applicable, and what responsibility does it assume for inputs, outputs, and third-party claims involving IP and personality rights?	Inventory of assets/licenses/authorizations, where applicable; representations and warranties clauses; allocation of responsibility matrix for inputs and outputs; indemnification obligations; limitations or exclusions of liability; claims clearance and response workflow
Incident response	Is there an emergency plan and channel? Notification deadline?	Playbook; SLA; contacts

RECOMMENDED PROCEDURE

- Request evidence (not merely “statements”) and require documentation of the tools/versions used and their intended purposes
- Require a human review workflow and approval criteria proportionate to the risk and type of campaign
- Include an SLA for correction/removal measures and establish an emergency communication channel
- Do not engage agencies based solely on a “creative portfolio” without reviewing processes and supporting evidence
- Do not accept “black-box” arrangements (i.e., no list of tools, no human review, and no traceability)
- Do not treat incidents as unlikely or remote consequences
- Assess in advance whether the agency/vendor assumes responsibility and indemnification obligations proportionate to the risks associated with AI-generated or AI-assisted outputs especially in cases involving third-party claims related to Intellectual Property and personality rights.

6.3 Internal policies and training

Internal policies translate principles into simple rules: what is permitted or prohibited, who is responsible for approvals, how records should be maintained, and how questions or concerns should be escalated. Continuous training reduces operational risks (e.g., the use of confidential information in prompts) and strengthens the ability to critically review outputs, particularly in sensitive matters.

RECOMMENDED PROCEDURE

- Define in writing which information/data may be entered into AI systems
- Require evidence of ongoing training and, where applicable, a governance structure (designated responsible person/committee)
- Use checklists and approval gates for AI-related activities (creative, media, customer service, research)
- Do not rely on “common sense” as a policy: without clear guidelines, teams will act inconsistently and risks will increase
- Do not allow the adoption of tools without minimum vetting (security, privacy, IP)
- Conduct periodic training sessions and ensure that practices and materials remain up to date
- When developing an AI Policy for Marketing, address: scope and objectives; roles and approval processes; rules regarding permitted data and information; approved tools and prohibited uses; transparency toward the public; human review requirements and checklists; traceability and evidence retention; incident management; and periodic training and updates

6.4 Selection and approval of tools

Approving a tool means validating, before its use, whether it is appropriate for the level of risk involved in the campaign and compatible with the advertiser’s requirements (security, privacy, Intellectual Property, transparency, and traceability). In practice, this means pre-approving which systems may be used, requiring assessments proportionate to the complexity of the campaign, and ensuring traceability mechanisms (such as date, prompts, logs, and model versions), as well as human review processes.

MINIMUM APPROVAL CHECKLIST (EXAMPLE)

Criteria	What to check / record
Purpose	For what purpose the tool will be used (creative, media, customer service, etc.) and applicable limitations
Input data	Whether personal/confidential data will be used; anonymization rules; prohibitions
Training using prompts	Whether there is an option to disable the use of prompts/inputs for training purposes; default settings
Security	Controls (access, MFA, logs, encryption), and evidence (ISO/SOC 2, where available)
IP and licenses	Rights relating to outputs; limitations regarding datasets/training; documentation of origin/licenses where applicable and proportionate to risk; contractual provisions with the vendor concerning representations, warranties, and indemnification in case of third-party rights violations
Transparency	Whether the tool allows labels/metadata/watermarks where necessary
Traceability	Date, prompt, generation logs, model version, responsible person, approvals
Availability	Assurances regarding system availability and the existence of SLAs

PRACTICAL SUGGESTION

Maintain an internal inventory of tools (name, vendor, approved purpose, responsible person, mapped risks, and date of the last review).

6.5. Governance Gate Before Go-Live

As a practical implementation of the guidelines above, it is recommended that campaigns involving the use of AI undergo, prior to go-live, a formal governance gate proportionate to the risk level of the use case, with integrated participation from the marketing, legal, privacy, and compliance teams, without prejudice to the involvement of other areas when necessary.

This gate should function as a minimum validation checkpoint before publication, confirming whether the campaign meets the applicable requirements for compliance, integrity, transparency, traceability, and incident response appropriate to its level of risk.

The gate should not be treated as a bureaucratic formality, but rather as a minimum coordination mechanism among teams, capable of ensuring consistency in decision-making, accountability, and prompt response in cases of content correction, removal, or incidents.

6.6 Operational workflow with AI (end-to-end)

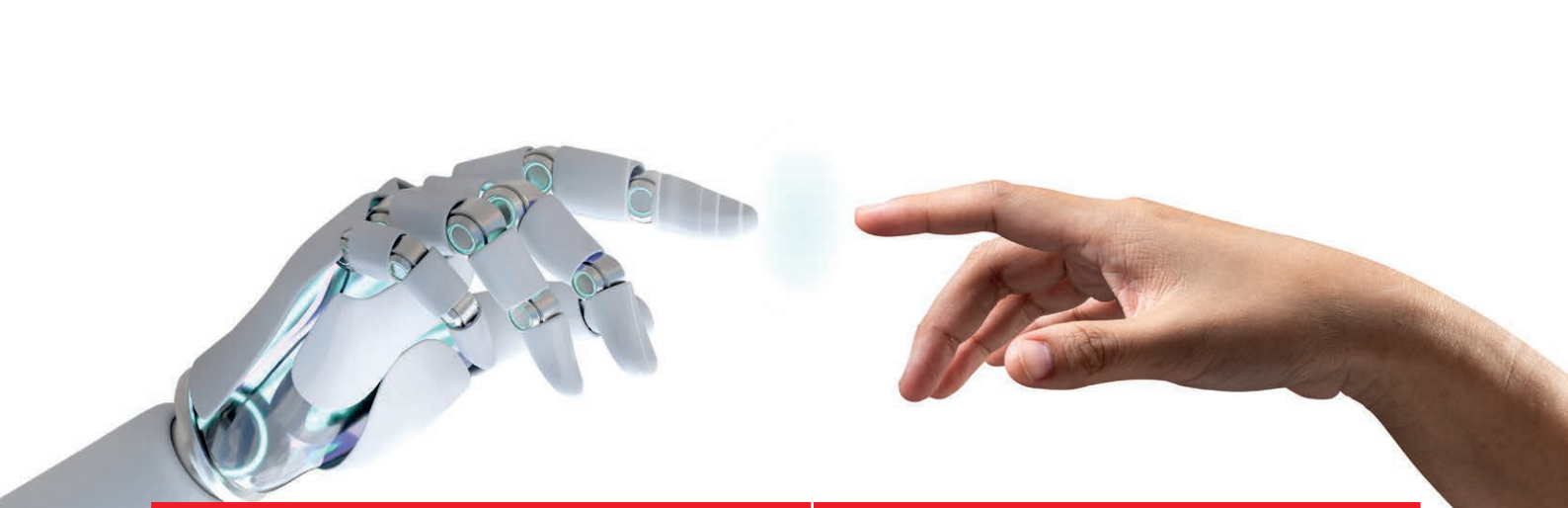
An end-to-end workflow should define stages, mandatory reviews, evidence retention requirements, and deadlines for correction/removal measures, while also establishing clear levels of human review prior to publication, records of reviews/approvals, and SLAs for corrections, rectifications, and content takedown whenever risks arise.

The workflow below represents a minimum operational framework. It enables the efficient use of AI without compromising traceability, review processes, and readiness for correction. The governance gates should be adjusted according to the level of risk involved (see Section 4.8 – proportionality of this guide).

Stage	Minimum Control	Primary responsible party
1. Briefing and scope	Define the purpose, audience, channels, and AI constraints	Advertiser and Agency
2. Risk assessment	Classify the use case (low/medium/high risk) and disclosure requirements	Agency (with validation by the Advertiser)
3. Tool selection	Use approved tools and proper configuration	Agency / Vendor and Advertiser (approval)
4. Input preparation	Check personal data, trade secrets, and Intellectual Property issues; apply policies	Agency
5. Generation/production	Record prompts/ versions, and relevant parameters	Agency and Vendor
6. Human review	Creative and legal review proportional to risk	Agency and Advertiser
7. Governance gate before go-live Clearance and approvals)	Rights (IP/persona), claims and disclosures defined; final consolidation of internal validations; prior review and approval by the advertiser before publication or delivery of outputs generated or substantially modified by AI, proportionate to the risk of the content	Advertiser (final decision-maker), with validation by the relevant internal teams
8. Publication	Configure segmentation/optimization settings and record changes	Agency
9. Monitoring	Monitor performance, biases, complaints, and anomalies	Agency and Advertiser
10. Closure	Retain evidence and lessons learned; update controls accordingly	Advertiser and Agency

6.7 Traceability and documentation

Traceability is the ability to reconstruct the how and why behind a piece of content or a decision: which inputs were used, which tool/model was applied, who reviewed and approved it, and which controls were implemented. In marketing, this is essential to demonstrate due diligence, respond to complaints, and correct issues quickly.



MINIMUM CAMPAIGN RECORDS	WHAT IT IS USED FOR
Use case; tool/model (name, version) and date	Identify what was used and when
Responsible parties and approvals (agency/advertiser)	Accountability and decision trail
Relevant inputs (sources, datasets, creative assets) and restrictions	Control of IP, confidentiality, and LGPD
Key prompts/parameters and versions of generated assets	Reproducibility and incident investigation
Disclosure decision (if applicable) and justification	Avoid material omission and label fatigue
Tests and validations performed (bias, claims, quality)	Evidence of risk mitigation
Relevant operational logs (when available)	Anomaly detection and auditability

PRACTICAL SUGGESTION

Where third parties (agency/subcontractor) are involved, include a contractual obligation to maintain and provide documentation in the event of any inquiry or challenge.

6.8 Incident management and rapid response

AI-related incidents may include: publication of misleading or discriminatory content; infringement of rights (Intellectual Property, image/voice rights); leakage or exfiltration of information via prompts; or security failures by the provider.

AI incidents are not always “classic personal data incidents.” In addition to data breaches and unauthorized access (see Section 5.7 of this guide), algorithmic, reputational, and content-related incidents are also common (such as offensive outputs, bias, hallucinations, misuse of avatars/synthetic personas, or violations of personality rights). Sector guidelines recommend clear response and documentation protocols to reduce harm and demonstrate diligence.

Incident Type	Examples	Immediate Response Actions (first hours)	Escalation
Personal data (LGPD)	Data exposure, prompts containing personal data, unauthorized access	Contain (revoke access), preserve evidence, and notify DPO/security	Assess the need for notification and corrective measures
Content and reputation	Offensive content, stereotypes, unauthorized deepfake, improper use of voice/image	Pause distribution, remove/rectify content, record versions, and involve legal and PR teams	Review processes, issue clarifications, and remedy damages where applicable
Algorithmic (biases and decisions)	Exclusionary segmentation, optimization reinforcing disparities	Suspend rule/model, investigate parameters and data, and test corrections	Update criteria, monitor, and document actions taken
Information integrity	Chatbot hallucination, inappropriate response, incorrect claim	Interrupt workflow, correct dataset/guardrails, and guide support	Review content and validations; communicate when there is impact
Third parties and vendors	Term changes, service failure, vendor data breach	Activate SLA, require notification and containment plan, and assess replacement	Audit, adjust contracts and controls; report internally

The response must be fast, include an emergency channel, notification timelines, and an initial action plan, including removal/correction of content and preservation of evidence.

RECOMMENDED CONDUCT

- Define channels and responsible parties (marketing, legal, IT, DPO, PR) and conduct periodic simulations
- Quickly pause campaigns when there is material risk; preserve evidence (versions, prompts, logs)
- Treat AI incidents also as reputational and content-related incidents, with communication aligned with stakeholders
- Perform post-incident review (“post-mortem”) and adjust policies, tools, and training accordingly
- Do not minimize incidents as “AI errors” or rely solely on individual “common sense” for decisions
- Do not wait for full confirmation when there is risk of immediate harm to consumers
- Do not delete records without preserving evidence (as it undermines correction, auditing, and defense)
- Do not repeat the same type of failure without reviewing controls and responsibilities

Conclusion

The combination of personal data and AI is one of the main drivers of innovation in marketing — and, for this reason, it must be accompanied by responsibility, transparency, and effective governance. This Good Practice Guide brings together concepts, use cases, principles, risks, and safeguards with a focus on practical application, supporting advertisers, agencies, platforms, and vendors in adopting AI in a way that is both useful for the market and consistent with the protection of consumers, data subjects, and third-party rights.

More than a conceptual guide, this content is designed as a governance and due diligence instrument for advertisers. It can be used to structure internal policies, define roles and responsibilities, guide approval workflows, establish objective criteria for transparency/disclosure, and record minimum compliance evidence. It also serves as a reference for contracting, onboarding, and evaluating vendors, translating conduct expectations into clauses, checklists, and verifiable routines.

Effective implementation depends on minimum commitments: defining purposes and limits, maintaining human oversight, ensuring traceability, promoting transparency when relevant, and operating with readiness to correct failures and incidents. By adopting these routines, the advertising ecosystem strengthens trust, reduces regulatory and reputational risk, and enables innovation and compliance to advance together.

In this sense, the Good Practice Guide also supports qualified dialogue with authorities and stakeholders, demonstrating effective self-regulation practices and a commitment to continuous improvement.

Finally, it is a living instrument: it guides current practice and should be updated as technologies, practices, and regulatory references evolve.



About ABA

The ABA (Brazilian Association of Advertisers) is a non-profit organization founded in 1959. It brings together and represents the largest advertiser companies in Brazil, responsible for approximately 70% of all advertising investment in the country. The organization was created to represent and defend common interests and to contribute to the continuous development and professionalization of advertiser companies.

Its core mission is advocacy, focusing on defending freedom of commercial communication, representing, protecting, and guiding Brazilian advertisers, and maintaining an ongoing dialogue with society and its various stakeholders. The Association is also a founding member of CONAR, reinforcing self-regulation as a key instrument for integrity and trust in advertising. On the international stage, ABA is part of the Executive Committee of the WFA (World Federation of Advertisers), connecting Brazil's agenda with global best practices.

Through technical forums and working groups — such as the AI Working Group and the Privacy and Data Protection Working Group — ABA develops principles, guidelines, and initiatives aimed at strengthening sector self-regulation and supporting responsible innovation in marketing and advertising.

Among the leaders who contributed to this Guide, we highlight:

- Lucas Gobbo, Co-leader of the ABA Privacy and Data Protection Working Group and Global Legal Manager & Product Counsel at BEES - AB InBev
- Paula Ercole Bauléo, Leader of the ABA Artificial Intelligence Working Group and Senior Legal Manager at General Mills
- Rodrigo Borges, Leader of the ABA Privacy and Data Protection Working Group and Director of Privacy – Latin America at Kenvue

About VLK

VLK is a boutique law firm specializing in Digital Law, Data Protection, Cybersecurity, Artificial Intelligence, and Legal Marketing, driven by deliverables that make a real difference.

At VLK, law is not seen as a barrier. It is a driver of innovation, enabling business development and contributing to a more prosperous and fair society by reconciling risk and opportunity, complexity and clarity, as well as protection and progress. We actively participate in the development of regulatory frameworks and are involved in numerous innovative and strategic projects, which allows us to anticipate trends and provide legal certainty.

Among the professionals from the firm who contributed to this Guide, we highlight:

- Rony Vainzof – Partner
- Gisele Karassawa – Partner
- Mariana Carlucci – Lawyer
- Jean Santana – Lawyer

SUPPORTED BY:



2030: The Future Passes Through Here.

Associação Brasileira de Anunciantes
aba.com.br
comunicacao@aba.com.br
+55 11 3283-4588

🌐 bit.ly/facebook-aba
📷 [instagram.com/abatransformar/](https://www.instagram.com/abatransformar/)
🌐 bit.ly/linkedin-aba

Member of WFA
World Federation of Advertisers



wfanet.org
info@wfanet.org
+32 2 502 57 40

📺 [youtube.com/wfamarketers](https://www.youtube.com/wfamarketers)
🌐 [linkedin.com/company/wfa](https://www.linkedin.com/company/wfa)