LEXOLOGY

Digital Law in Brazil - Hot Topics | Privacy Policy Must-Haves Under Brazil's LGPD: Legal Requirements and Local Practice

Montaury Pimenta, Machado & Vieira de Mello

Brazil | February 23 2026

Under the Brazilian General Data Protection Law (LGPD), the Privacy Policy plays a central role in operationalizing the principles of transparency, purpose limitation, and accountability established in Article 6 of the law. Far from being a mere formality or a copy-and-paste document, as many organizations still rely on, the Privacy Policy is one of the primary instruments through which controllers demonstrate compliance to both data subjects and regulators.

In practice, Brazil's enforcement agency, the ANPD, has made clear that incomplete, generic, or outdated privacy notices significantly increase legal and regulatory exposure. This is particularly evident in the context of data subject complaints and administrative proceedings, where missing elements, such as the identification of the party responsible for data processing or the absence of a communication channel, have drawn regulatory scrutiny.

For this reason, understanding the essential elements that a Privacy Policy must contain, and how they are interpreted under local practice, is a critical step for any company or organization processing personal data in Brazil.

Identification of the Controller

Articles 6(VI) and 9 define who is collecting the data and must be clearly identified. Local practice recommends including the company's or entity's legal name, tax registry number (CNPJ), full address or city of headquarters, and where applicable a clarification regarding joint controllers. Given that transparency is a foundational LGPD principle, vague or incomplete identification should be avoided.

Data Collected

Articles 6(I) and 9 govern what types of data are processed. To demonstrate data minimization, best practice is to categorize data by type, such as identification, contact, behavioral, and technical data, while clearly distinguishing between personal data and sensitive personal data. Overly broad descriptions such as "personal data including name, email, and others" should be avoided, as they undermine the specificity the LGPD demands.

Purpose of Processing

Articles 6(I) and 7 require clarity on why and how data is used. Purposes should be specific, concrete, and expressly linked to their corresponding legal bases. While this alignment is not strictly mandatory under the law, it is strongly recommended in practice: it reduces interpretive ambiguity and substantially strengthens the controller's position in complaints before the ANPD or in litigation.

Data Sharing

Articles 9 and 33-36 address with whom data may be shared. The policy should clearly identify categories of recipients, such as payment processors, cloud providers, and marketing platforms, disclose whether international data transfers occur, and describe the safeguards adopted for cross-border transfers. Transparency remains paramount, even when listing recipient categories only rather than naming specific third parties.

Data Subject Rights

Article 18 sets out the rights data subjects may exercise, including access, correction, deletion, and withdrawal of consent. Best practices include specifying the channels through which requests can be submitted (email, online form, platform) and confirming that the policy covers core rights such as confirmation of processing, data access, and correction of incomplete, inaccurate, or outdated information.

Information Security

Article 46 requires that appropriate security measures be adopted. This section demands careful drafting: over-promising for instance, by listing specific technologies, can become a liability if those measures are not consistently applied. Preferred formulations include references to "technical and organizational measures," "access controls," "encryption where applicable," and "internal data protection policies," which convey commitment without creating undue legal exposure.

Storage and Retention

Articles 15 and 16 govern how long data is retained and when it must be deleted. Practical and precise drafting is essential here. The policy should clarify the applicable retention criteria whether based on legal obligations, contractual necessity, or legitimate interest, and note that deletion may, in certain cases, be replaced by anonymization. This framing should be aligned with Brazilian data retention realities across tax, consumer protection, and labor law frameworks.

Data Protection Officer (DPO) Contact Information

Article 41 makes DPO contact information mandatory. At minimum, the policy must include an email address and the title or function of the responsible party whether a formally appointed DPO or a designated data protection contact point. This remains one of the elements most frequently flagged in ANPD proceedings when absent.

Use of Cookies

Articles 6 and 9 apply to tracking and behavioral data collected through websites. A standalone Cookie Policy, referenced within the Privacy Policy, is both common and acceptable to the ANPD, which has aligned its approach with global practice in this area.

Policy Updates

Although not explicitly required by the LGPD, clearly indicating the date of the last policy review is strongly recommended. It reflects good governance and ongoing compliance commitment and can serve as a meaningful defense against claims that an outdated policy evidences negligence or indifference to data protection obligations.

A properly structured Privacy Policy aligned with the LGPD is not merely a local legal requirement, it is a cornerstone of a broader data governance and compliance strategy. From the clear identification of the controller to transparent disclosures regarding data collection, purposes, sharing, retention, and security measures, each component contributes to fulfilling the LGPD's accountability framework and to mitigating regulatory risk.

In the Brazilian context, the ANPD has consistently emphasized that transparency must be substantive, not merely formal. Privacy notices must accurately reflect actual data processing practices, not aspirational or generic descriptions of what a company might do. Organizations should therefore treat their Privacy Policy as a living document: periodically reviewed, aligned with internal procedures, and capable of bridging legal compliance, operational reality, and trust with data subjects.

Montaury Pimenta, Machado & Vieira de Mello - Pablo Torquato

Montaury Pimenta, Machado & Vieira de Mello is a Leading Brazilian Intellectual Property (IP) law firm, distinguished for its work in complex IP Litigation, IP Prosecution, and Enforcement. Click here to learn more about the firm **https://www.montaury.com.br/en/**