

CONTRACT NEGOTIATION



To ensure compliance with applicable legislation and reinforce the company’s commitment to data protection, it is essential that every contract involving the processing of personal data be carefully reviewed.

The checklist below outlines key points to consider in this task. Depending on negotiation and the characteristics of the parties involved, other topics may also need to be considered.

☐

Subject Matter

Does the contract clearly define its subject matter? Is it possible to understand the need for personal data processing to achieve this purpose?

☐

Role of the Parties

Does the contract define the role of each party as data processing agents – such as controller, processor, or sub-processor? Are the responsibilities and the level of autonomy of the parties clearly outlined?

Note: identifying each party’s role is crucial for determining applicable responsibilities and obligations. For more information, see the ANPD’s [guide for defining data processing agents and the data protection officer](#).

☐

Purpose of Processing

Does the contract clearly specify the purposes for which personal data may be processed by each party? Are there defined restrictions and possible consequences for non-compliance with such purposes?

Note: contracts between controllers and processors should reference the instructions, recommendations, and guidelines provided by the controller.

☐

Legal Basis

Does the contract specify who is responsible for defining the legal basis for personal data processing?

Note: the LGPD assigns different responsibilities to controllers and processors. It is essential that the contract reflects these responsibilities.



Data Subjects’ Rights

Does the contract clearly define each party’s responsibilities regarding the handling of data subjects’ requests?



Data Sharing

Does the contract establish limitations and conditions for sharing personal data with third parties? Are there clauses defining the necessary safeguards to protect the shared data?



Security

Does the contract detail the security measures that must be implemented to protect personal data? Is there a clause outlining the deadlines and procedures for notifying security incidents between the parties?

Note: The Security Incident Communication Regulation ([Resolution CD/ANPD No. 15/2024](#)) requires that incidents posing a risk or significant harm to data subjects be reported to the ANPD and to the affected data subjects within 3 business days.



Data Deletion

Does the contract clearly specify the conditions that trigger the obligation to delete or return personal data, as applicable? Does the contract detail the procedures to be followed by the parties, including the provision of deletion evidences?



Liability and Indemnification

Is liability for damages related to improper data processing clearly defined? Are there distinctions between direct and indirect damages? Are there liability limitation clauses that affect data protection-related issues?