

PRIVACY POLICY AND DATA PROTECTION

INDEX

I. Objective	3
II. Glossary	3
III. Principles for the Processing of Personal Data	5
IV. Responsibilities	6
V. Legal Bases for the Processing of Personal Data	9
VI. Data Sharing.....	10
VII. Security of Personal Data	11
VIII. Storage and Disposal of Personal Data	11
IX. Rights of Data Subjects.....	12
X. Activities of Personal Data Processing	13
The following procedure should be observed to safeguard the Data Subject's rights:	15
XI. Policy Violations	18
XII. Data Protection Officer Information	19
XIII. Update and Validity.....	19

I. Objective

O GT Lawyers ("GT") carries out its legal activities with a high level of commitment to its partners, lawyers, interns, and employees ("Collaborators"), clients, suppliers, and partners, particularly concerning the preservation of the right to privacy and the protection of Personal Data of all individuals.

Therefore, this Privacy Policy and Data Protection ("Policy") aims to regulate the processing of Personal Data by GT, protecting the fundamental rights of freedom and privacy of each individual.

This Policy will cover all Personal Data processed in the development of GT's activities.

II. Glossary

In order to facilitate the understanding of this Policy, the following concepts are defined:

Personal data: any information related to a natural person that allows their identification or makes them identifiable.

Sensitive personal data: data linked to a natural person about racial or ethnic origin, religious belief, political opinion, membership in a union or organization of a religious, philosophical, or political nature, data relating to health or sexual life, genetic or biometric data.

Data Processing Agents: they are the Controller and the Processor. Anonymization: use of reasonable and available technical means at the time of Processing, through which data loses the possibility of direct or indirect association with an individual.

National Data Protection Authority ("ANPD"): a public administration body responsible for overseeing, implementing, and enforcing compliance with the LGPD throughout the

national territory. Controller: natural or legal person, public or private, to whom decisions regarding the Processing of Personal Data belong.

Anonymized data: data relating to the Data Subject that cannot be identified, considering the use of reasonable and available technical means at the time of its Processing.

Data Protection Officer: person appointed by the Controller or Processor to act as a communication channel between the Controller, the Data Subjects, and the National Data Protection Authority ("ANPD").

LGPD: Law No. 13,709/2018, which came into force on September 18, 2020.

Processor: natural or legal person, public or private, who carries out the Processing of Personal Data on behalf of the Controller.

Data Subject: natural person to whom the Personal Data being processed refer ("Data Subject").

Processing: includes all operations or set of operations carried out with Personal Data, whether by automated means or not, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, disposal, assessment, information control, modification, communication, transfer, dissemination, and/or extraction.

III. Principles for the Processing of Personal Data

With the aim of guiding the Processing of Personal Data, the LGPD established several principles that will assist in the interpretation of this Policy:

Principle	Definition	In this case, it should be asked:
PURPOSE	The Processing of Personal Data should only occur to achieve legitimate purposes, with the purpose being specified and expressly informed to the Data Subject.	Why are these data being processed?
ADEQUACY	Compatibility of the Processing with the purposes informed to the Data Subject and the activities effectively carried out.	Are the data being processed for the purpose previously agreed upon/informed to the Data Subject?
NECESSITY	Personal Data Processing should be minimized to the extent necessary.	Are all these data truly necessary for carrying out the activities?
FREE ACCESS	Assurance given to Data Subjects of easy and free consultation regarding the manner and duration of Processing their Personal Data.	At GT, can the Data Subject exercise their rights, including accessing their data in a straightforward and swift manner?
DATA QUALITY	The Personal Data processed must be maintained with accuracy, clarity, relevance, and updated as necessary to fulfill the purpose of their Processing.	Does GT take care to verify and confirm the accuracy of the Personal Data collected?
TRANSPARENCY	Clear, accurate, and easily accessible information about the Processing must be provided to Data Subjects, while observing commercial and industrial secrets.	Is the information provided to Data Subjects delivered with clarity and transparency?
SECURITY	Utilization of technical and administrative measures capable of protecting Personal Data from unauthorized access and/or	Is GT adopting appropriate security measures to protect Personal Data?

	accidental, unlawful destruction, loss, alteration, dissemination, or leakage.	
PREVENTION	Need for adopting measures to prevent the occurrence of damages due to the Processing of Personal Data.	Is there any measure I can take to, for example, mitigate risks against data breaches?
NON-DISCRIMINATION	Do not use Personal Data for unlawful or abusive discriminatory purposes.	Is the Processing of Data disadvantaging a certain type of person?
ACCOUNTABILITY	Demonstration of the adoption of effective measures that demonstrate compliance with Personal Data protection regulations.	How does GT demonstrate that it has adopted effective measures and is in compliance with the law?

IV. Responsibilities

In full compliance with the LGPD, all employees, suppliers, clients, and partners of GT have their respective level of responsibility regarding the manner in which they carry out the Processing of Personal Data in the performance of their activities, with each of them being responsible for observing and enforcing this Policy and all legal principles for the Processing of Personal Data as provided by law.

Among the main responsibilities related to Privacy and Data Protection within **GT's** corporate environment, we can mention:

A. PARTNERS/UPPER MANAGMENT

The partners will be directly responsible not only for the process of GT's compliance with current legislation but also for maintaining compliance with applicable personal data protection laws, demonstrating engagement with an ethical and integral posture to reinforce

the importance of this commitment to the firm and support all actions necessary for the implementation of an effective privacy and personal data protection program. Therefore, the commitment of the partners and, consequently, of GT's upper management is an indispensable condition for the cultural integration of all employees.

B. DATA PROTECTION OFFICER

The Data Protection Officer will be the person responsible for monitoring and ensuring that GT complies with the privacy and data protection rules established by law, acting as a channel of communication between GT, Data Subjects, and the ANPD (National Data Protection Authority). They will operate with full autonomy and report all matters related to the subject to the Partners/Upper Management.

Their primary responsibilities include:

- Map, develop, and create processes, flows, procedures, and protocols related to the area of data protection and privacy and manage GT's compliance process with the LGPD;
- Receive requests, complaints, and communications from Data Subjects, provide clarification, and take appropriate measures to ensure that their rights are respected;
- Receive communications and notifications from the ANPD and any other body or agency related to Personal Data Protection, provide the necessary clarifications through documents, as well as take any and all necessary measures;
- Guide clients, Collaborators, and partners regarding the practices to be adopted concerning the protection of Personal Data;
- Review impact reports on personal data protection periodically and whenever requested by the ANPD, which will be prepared by the area responsible for data processing;
- Maintain and manage the record of Personal Data Processing operations carried out by GT, especially when based on legitimate interest;
- Assist the partners in the decision-making process regarding privacy and personal data protection, as well as communicate about any processes and protocols adopted that

represent risks to privacy and personal data protection, assisting in the development of solutions and ways to mitigate such risks;

- Guide and assist the Partners and GT's press office in the event of an information security incident;
- Guide GT's areas in choosing service providers and commercial partners to ensure that they are duly compliant with the LGPD;
- Propose and coordinate periodic update training sessions for GT's Collaborators, suppliers, and partners on the LGPD;
- Monitor and supervise the application and effectiveness of the Data Protection compliance program, as well as new regulations and/or guidelines to be published by the ANPD.

C. PRIVACY AND DATA PROTECTION COMMITTEE ("PDPC")

The PDPC will be a permanent and multidisciplinary advisory body that will support the Data Protection Officer in carrying out privacy and data protection routines, coordinating and overseeing GT's compliance process with the LGPD, and working on the development of standards and best practices to ensure proper handling of personal data by the firm, in accordance with the law.

GT's PDPC will be comprised of the Data Protection Officer and representatives from the areas to be defined in the respective Appointment Act by the equity partners, whose main responsibilities are as follows:

- Propose policies and suggest awareness actions for all internal agents involved in Personal Data Processing by GT;
- Discuss and participate in the development and updating of standards, policies, reports, and documents related to Personal Data Processing by GT;
- Manage activities related to Personal Data Processing by GT;
- Oversee the implemented governance program and supervise processes involving Personal Data Processing;

- Request information from GT areas as well as investigations when there is suspicion of information security incidents;
- Resolve any doubts from Collaborators and third parties and advise on matters related to data protection.
- Manage incidents and crises related to Personal Data Processed by GT;
- Create a response plan upon identification of incidents and crises, including information security incidents concerning the Personal Data Processed, as well as establish protocols for damage containment in such situations;
- Develop methods for incident and crisis recovery;
- Define actions to mitigate risks in case of incidents and crises;
- Prepare incident and crisis reports, and review applicable procedures;
- Adopt corrective measures, normative adjustments, and procedural adaptations necessary to prevent situations of vulnerability to the security of the Personal Data Processed.

D. EMPLOYEES, CLIENTS, SUPPLIERS, AND PARTNERS

Every professional, whether an employee, supplier, client, or partner, plays a fundamental role in ensuring that the Processing of Personal Data occurs in a legitimate, secure, and lawful manner. This means that privacy and protection of Personal Data are the responsibility of all, who must prioritize and commit to acting in accordance with the best security practices and ensuring compliance with legal duties regarding Data Processing and the full exercise of Data Subjects' rights.

V. Legal Bases for the Processing of Personal Data

GT will process Personal Data solely in accordance with the legal bases provided for in the LGPD, and the Data Protection Officer should always be consulted when there is doubt about the legal basis to be used to justify the Processing.

Below are the main legal bases that may be used by GT:

- **CONSENT:** when the Data Subject expressly and unequivocally expresses their will for a certain Personal Data Processing activity to occur;
- **COMPLIANCE WITH LEGAL OR REGULATORY OBLIGATION:** when Processing is necessary to comply with a legal or regulatory obligation;
- **PERFORMANCE OF A CONTRACT OR PRELIMINARY PROCEDURES WITH THE DATA SUBJECT:** when necessary for the provision of a service, supply of a product, or functionality requested directly by the Data Subject, even before effective contracting;
- **JUDICIAL, ADMINISTRATIVE, OR ARBITRAL PROCESS:** when Processing is necessary for the defense of GT's interests in a litigation situation;
- **LEGITIMATE INTEREST:** when necessary to meet GT's or third parties' legitimate interests, except where the fundamental rights and freedoms of the Data Subject requiring the protection of Personal Data prevail.

VI. Data Sharing

GT may share Personal Data with accounting and human resources service providers, as well as software and systems providers, for the purpose of managing records, documentation, and other necessary arrangements.

It may also share Personal Data with business partners (national and international), correspondents, experts, auditors, accountants, translators, and others when necessary to assist in the legal activities provided by GT.

For any form of sharing, legal requirements and necessary procedures will be respected to ensure that the process occurs legitimately. In the case of international data sharing, Employees should observe the need to prepare and sign contracts or commitments containing clauses for the protection of personal data.

VII. Security of Personal Data

GT will adopt, in accordance with the LGPD, security measures, technical and administrative, capable of protecting Personal Data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, leakage, implementing, if necessary, additional security measures adequate to the technical standards to be set forth by the ANPD in the future.

In this sense, GT will adopt security standards established in applicable laws and regulations, such as: (a) Training, governance, internal security policies; (b) Control of storage on its own or contracted servers; (c) Protection against unauthorized access; (d) Authorized access only to specific individuals to the location where their personal information is stored, provided that such access is essential to the development of the intended activity; (e) Confidentiality of professionals accessing the information/data; (f) Application of administrative, disciplinary, and legal sanctions applicable to Employees and individuals who improperly use their information, in violation of this Privacy and Data Protection Policy; (g) Absolute commitment to the principles set forth by the applicable legislation, as well as to the storage and deletion of data, the latter when requested;

All Personal Data provided will have access limited to qualify and duly authorized agents to process them, in strict accordance with the purposes mentioned in this Policy, and even after the end of its Processing, GT undertakes to notify the ANPD and the Data Subject in the event of any security incident that may entail relevant risk or damage to the Data Subjects.

VIII. Storage and Disposal of Personal Data

GT will store Personal Data for the entire duration of the Processing, and afterwards, they will be discarded and/or anonymized (except those maintained as required by law), in compliance with Article 16 of the LGPD.

Personal Data of Data Subjects will not be kept in GT's database for longer than necessary for the purposes for which they were collected or otherwise processed, subject to the legal permissions and restrictions relevant to the subject.

For this purpose, GT will periodically analyze, through its Data Protection Officer, the maintained database, with proper evaluation of the justifications provided by the areas, in order to avoid situations of excessive or unnecessary Processing of Personal Data, or Processing conducted in non-compliance with the legislation.

IX. Rights of Data Subjects

Data Subjects will be granted all applicable rights, in accordance with legal requirements, the compliance of which will be monitored by the Data Protection Officer with the support of the Privacy and Data Protection Committee (CPPD). These rights include:

1. **CONFIRMATION OF THE EXISTENCE OF TREATMENT:** The Data Subject can inquire whether their Personal Data is being processed by GT.
2. **ACCESS:** The Data Subject can request information about the existence of their Personal Data in GT's database and, if it exists, may also request access to their Personal Data, including information about the data's origin, the criteria used, and the purpose of the processing.
3. **CORRECTION:** The Data Subject can request the correction of their information when it is incomplete, inaccurate, or outdated.
4. **ANONYMIZATION, BLOCKING, OR ELIMINATION OF UNNECESSARY DATA:** The Data Subject can request the anonymization, blocking (for certain purposes), or even the elimination of their Personal Data if they believe it to be unnecessary or excessive for specific purposes or if it is being processed unlawfully.

5. **ELIMINATION OF PERSONAL DATA PROCESSED WITH CONSENT:** In some cases, the Data Subject may request the deletion of their Personal Data, subject to legal and regulatory obligations.
6. **INFORMATION:** The Data Subject may request information about the processing of their Personal Data.
7. **INFORMATION ABOUT NON-PROVISION OF CONSENT:** The Data Subject can inquire about the consequences if they do not consent to the processing of their Personal Data.
8. **REVOCATION OF CONSENT:** The Data Subject may, at any time, request the revocation of previously given consent.
9. **OBJECTION:** The Data Subject may object to the processing carried out on the basis of one of the exceptions to the requirement for consent.

X. Activities of Personal Data Processing

A. RECORD OF ACTIVITIES

Every operation involving the processing of Personal Data will be recorded and documented, especially when based on legitimate interest.

Each area of GT will be responsible for keeping records, with oversight from the DPO.

The records should be updated every six months by GT's areas, which will be responsible for filling out and ensuring the accuracy of the recorded information. Based on the records, the DPO will identify any non-conformity in activities with data protection legislation and request the necessary corrections/adjustments.

B. PRIVACY IMPACT ASSESSMENTS AND RISK ASSESSMENTS

The DPO will review the legal bases indicated by GT's areas to assess activities that impact the rights and freedoms of the Data Subject and the potential risks they may pose to their privacy.

C. FITTING OF NEW PROJECTS (PRIVACY BY DESIGN)

For each new activity or project, GT will evaluate the risks it poses to privacy and data protection. Depending on the level of risk, the new project: (i) will proceed without opposition; (ii) will require approval from the Partners to proceed, taking into account the DPO's opinion.

D. DATA PROTECTION IMPACT ASSESSMENT REPORT (DPIA)

The Data Protection Impact Assessment Report should be prepared whenever there is a risk of violating the rights of the Data Subject in a particular activity, especially in cases of processing activities based on legitimate interest or involving sensitive Personal Data.

E. RESPONSE TO PRIVACY INCIDENTS

In the event of a suspected security incident, i.e., any event that may compromise the confidentiality, integrity, and availability of Personal Data, GT must follow the procedure outlined in item F below, which will be specifically created for this purpose.

F. RESPONSE TO DATA SUBJECT REQUESTS

Responding to a Data Subject's request regarding their rights under Article 18 of the LGPD should be done in a free, prompt, and effective manner. To this end, requests should be addressed by the DPO (via email), and should:

- (i) Upon receiving the request, acknowledge receipt within a maximum of 48 (forty-eight) hours;
- (ii) Subsequently, the DPO should respond to the Data Subject within a maximum of 15 (fifteen) days from the date of receiving the request, assuming there are no additional pending information to be provided by the Data Subject.

The following procedure should be observed to safeguard the Data Subject's rights:



f.1. Types of Data Collected and How We Use That Data

When you access and use our website, engage our services, provide services to us, or interact with GT in any way, we may process your personal data for various purposes, including some examples indicated below:

Data Collected	Purposes
Contact Information (name, email, organization, job title, phone number, address).	• To address your inquiries, compliments, complaints, suggestions, and communicate with you, especially when you send us a message through the Contact page on our website. • To manage our relationship with you or with the company you represent, if you are a client, former client, or potential client. • For conducting meetings, whether in person or virtually, telephone discussions, or general discussions. • For managing billing and invoicing for our fees, costs, or expenses related to the legal services contracted by you or the company you represent.
Information provided on your resume (name, address, phone number, email).	• To evaluate the alignment of your professional profile with open job positions.

Qualification data (full name, nationality, marital status, profession, address, ID card, CPF (Brazilian taxpayer ID), driver's license, email address, passport).

- To draft, review, or negotiate contracts in which you are one of the parties, a representative of the parties, or otherwise involved.

- For the handling of administrative or legal proceedings in which you are one of the parties, a representative of the parties, or otherwise involved.

- For conducting legal due diligence to assess an organization's compliance with Brazilian legislation and risk evaluation, especially in mergers and acquisitions, corporate restructurings, or capital market transactions.

- To draft, review, or negotiate legal instruments or documents required in accordance with applicable legislation.

f.2. Who Your Personal Data is Shared With?

We may share your personal data with:

- **GT Offices:** We may share your personal data among GT offices in Rio de Janeiro, São Paulo, or any offices subsequently opened by GT, to enhance our services and gain efficiency in our business operations, such as using unique or integrated systems among our offices.
- **Our partners, service providers, and suppliers:** To carry out our activities, we maintain relationships and contract various partners, service providers, and suppliers, essential to our business. Some of these partners, service providers, and suppliers may need to access the personal data we collect to perform their functions, such as IT service providers, data hosting services, paralegals, auditors, correspondents, translators, among other service providers, in which case we may share your personal data with them.
- **Government Authorities:** We may share your personal data with any Government Authority that requests it, including labor or financial activities oversight bodies, regulatory agencies, judiciary bodies, Federal Revenue Service, or Police Authorities.
- **Third parties indicated by you:** We may share your personal data with third parties who have been indicated by you, upon your request.

XI. Policy Violations

In case of violation of this Policy or legislation, the facts will be investigated through appropriate methods, and disciplinary or corrective measures will be applied, proportionally to the severity of the event, in compliance with labor legislation and other investigation procedures to be promptly communicated to the employees, ensuring the right to full

defense and due process. If any situation indicating a violation of this Policy is identified, it must be immediately reported to the Data Protection Officer.

XII. Data Protection Officer Information

In case of doubts and/or requests regarding Privacy and Data Protection, please contact the Data Protection Officer of GT via email, phone, or postal address:

- Name: Anne-Catherine Brunschwig;
- Mailing Address: Rua Ataulfo de Paiva, 135 - Suíte 410, Leblon, Rio de Janeiro – RJ, CEP: 22440 901;
- E-mail: compliance@gtlawyers.com.br;
- Phone: (21) 25407282.

XIII. Update and Validity

This Policy is effective immediately and may be updated without notice and as needed. Updates will be made in our virtual environments.

Below are details about the current version of the Policy:

Document	Privacy and Data Protection Policy
Update Date	11/04/2024
Version	1.2
Approval Authority	Anne-Catherine Brunschwig
Signature	