PERSONAL DATA PROTECTION POLICY

July 2026

RECORD OF AMENDMENTS			
Version	**Item Amended**	**Amendment**	**Date**
1	Original version	-	01/2021
2	Addition of items	Addition of new topics	09/2022
3	General revision	General revision	07/2026

Table of Contents

1. General Definitions **1.1** Purpose and Scope **1.2** Regulatory Framework **1.3** Key Definitions and Responsibilities	4
2. Processing of Personal Data by Tera **2.1** Principles Applied to the Processing of Personal Data **2.2** Sources of Personal Data 2.2.1. Personal Data Received Incidentally or Unsolicited **2.3** Purposes of Processing and Legal Bases for the Processing of Personal Data 2.3.1. Legal Bases Not Applicable to Tera's Activities **2.4** Specific Requirements by Legal Basis 2.4.1. Compliance with a Legal and/or Regulatory Obligation (art. 7, II, LGPD) 2.4.2. Performance of a Contract and Preliminary Procedures (Art. 7, V, LGPD) 2.4.3. Regular Exercise of Rights (art. 7, VI, LGPD) 2.4.4. Legitimate Interest (arts. 7, IX, and 10, LGPD) 2.4.5. Consent (arts. 7, I, and 8, LGPD) **2.5** Shared Use of Data, Processors and Third Parties **2.6** Sensitive Personal Data **2.7** Recording of Meetings, Transcription and Artificial Intelligence Tools **2.8** Retention and Deletion of Personal Data **2.9** Record of Processing Operations and Impact Report **2.10** Security of Processing	8
3. Rights of Personal Data Subjects **3.1** Confirmation of Existence of and Access to Personal Data **3.2** Correction of Personal Data **3.3** Anonymization, Blocking or Deletion of Personal Data **3.4** Portability of Personal Data **3.5** Deletion of Personal Data Processed on the Basis of Consent **3.6** Information on the Sharing of Personal Data **3.7** Objection to Processing **3.8** Review of Automated Decisions **3.9** Information on the Refusal of Consent and Petition to the ANPD **3.10** Form of Request and Response Deadline	16
4. Response to Security Incidents **4.1** Purpose	18

4.2 Applicable Deadline **4.3** Internal Incident Response Workflow **4.3.1.** Overview **4.3.2.** Stages of the Workflow	
5. International Transfer of Data	20
6. Penalties **6.1.** Governance, Approval, Training and Review	22
7. Annexes 7.1. Communication Templates 7.1.1. Template for Communication to the ANPD 7.1.2. Template for Communication to Data Subjects	24

1. General Definitions

1.1 Purpose and Scope:

This Personal Data Protection Policy ("Policy") of Tera Investimentos Ltda. ("Manager" or "Tera") sets out the guidelines, responsibilities and procedures applicable to the processing of personal data in accordance with Law No. 13,709/2018, as amended ("Brazilian General Personal Data Protection Law" or "LGPD"), within the scope of the activities carried out by the Manager, without prejudice to any other measures that may be necessary for full compliance with personal data protection rules, such as the mapping of personal data processing activities and the assessment of the Manager's maturity with respect to personal data protection.

To this end, this Policy sets out the rules applicable to the mapping, collection, use, sharing, storage and deletion of personal data, as well as the governance measures necessary to ensure Tera's compliance with data protection legislation, and must be observed by all Personnel[1] in the performance of their duties.

The rules described in this Policy apply to all Processing of Personal Data carried out by the Manager, regardless of whether the data was provided by the Data Subject or obtained from third parties, public sources or reference databases, and cover, among others, investors or families with whom the Manager has a direct commercial relationship ("Clients" and "Prospective Clients"), natural persons related to suppliers, service providers and counterparties in the transactions of the portfolios under management ("Service Providers and Counterparties"), Personnel, or natural persons whose data is processed in the fulfillment of legal and regulatory due diligence duties, even if they have no relationship whatsoever with the Manager.

1.2 Regulatory Framework

This Policy is based on the rules and regulations indicated below, without prejudice to any others whose subject matter relates to the topics addressed herein:

(i) Brazilian General Personal Data Protection Law;
(ii) CVM Resolution No. 21/2021 ("RCVM 21");
(iii) CVM Resolution No. 50/2021 ("RCVM 50");
(iv) CVM Resolution No. 175/2022 ("RCVM 175");
(v) Law No. 9,613/1998 and Law No. 13,810/2019;
(vi) ANBIMA Code of Regulation and Best Practices for the Administration and Management of Third-Party Assets;
(vii) ANBIMA Rules and Procedures on Basic Duties;
(viii) CD/ANPD Resolution[2] No. 04/2023 ("RANPD 04");
(ix) CD/ANPD Resolution No. 15/2024 ("RANPD 15"); and
(x) CD/ANPD Resolution No. 19/2024 ("RANPD 19").
(xi) CD/ANPD Resolution No. 32/2026, which recognizes the European Union as an international organization with an adequate level of data protection; and
(xii) Law No. 12,965/2014 (Brazilian Internet Civil Rights Framework);

[1] As defined in the Compliance Manual.
[2] National Data Protection Agency.

1.3 Key Definitions and Responsibilities

The defined terms used in this Policy shall be construed in accordance with the definitions set out in this document, in other internal manuals and policies of Tera and, on a subsidiary basis, in the applicable legislation, in particular the LGPD.

Set out below are the main definitions to be observed in the application of this Policy:

Consent[3]	A free, informed and unequivocal statement by which the Data Subject agrees to the processing of their personal data for a specific purpose. In the context of the Manager, Consent is a residual and exceptional legal basis, applicable only to the situations and validity requirements set out in item 2.4.5 of this Policy. It may be revoked at any time, by means of a free-of-charge and facilitated procedure; generic authorizations are null and void, and Tera bears the burden of evidencing that Consent was duly obtained.
Personal Data[4]	Any information relating to an identified or identifiable natural person[5]. In the context of the Manager, this comprises identification data (e.g., name, ID card, individual taxpayer registry number, etc.), qualification data, asset-related data, financial data, investor profile analysis data and contact details of Data Subjects, collected in the course of the Manager's activities, such as, but not limited to, prospecting, registration, reputational analysis (*background check*) in the context of KYC[6], KYP[7] and KYE[8], wealth and asset management.
Sensitive Personal Data[9]	Personal Data concerning racial or ethnic origin, religious belief, political opinion, membership of a trade union or of a religious, philosophical or political organization, data concerning health or sex life, and genetic or biometric data, when linked to a natural person.
Anonymized Data[10]	Data relating to a Data Subject who cannot be identified, taking into account the use of reasonable technical means available at the time of its processing. In the context of the Manager, this applies, for example, to aggregate or statistical information extracted from client/investor databases for internal studies, management reports or submission of data to sector databases (e.g., ANBIMA),

3 As defined in art. 5, XII, of the LGPD
4 As defined in art. 5, I, of the LGPD.
5 As defined in art. 5, II, of the LGPD.
6 Know Your Client
7 Know Your Partner
8 Know Your Employee
9 As defined in art. 5, II, of the LGPD.
10 As defined in art. 5, III, of the LGPD.

	where there is no possibility of re-identifying the data subject, in which case the data ceases to be subject to the LGPD regime.
Database[11]	A structured set of Personal Data, established in one or more locations, in electronic or physical media. In the context of the Manager, these correspond to client/investor registration systems, regulatory obligation management platforms (compliance systems), portfolio management systems and other physical or electronic repositories that store Personal Data of Data Subjects.
Data Subject[12]	The natural person to whom the Personal Data subject to Processing refers (art. 5, V, of the LGPD). In the context of the Manager, this includes, without limitation: (i) **Clients and Prospective Clients:** individual investors and unitholders of the investment funds and vehicles under management, clients of discretionary portfolio management and wealth management services, and natural persons in the process of registration or prospecting, even if the relationship does not materialize; where the client is a legal entity or vehicle, its legal representatives, attorneys-in-fact, officers, partners and individual ultimate beneficial owners; (ii) **Family group members and beneficiaries:** members of the Client's family group and beneficiaries of wealth, succession, insurance or pension structures whose data is necessary for the structuring, review or implementation of such solutions; (iii) **Personnel and candidates**: partners, employees, interns and individual service providers of the Manager, as well as job candidates; and (iv) **Service Providers and counterparties**: natural persons related to service providers, suppliers and counterparties of the portfolios under management. (v) **Third parties subject to due diligence procedures:** natural persons whose data is processed in anti-money laundering routines, politically exposed persons screening, restrictive list searches and other reputational due diligence, even if they have no relationship with the Manager; and (vi) **Visitors:** natural persons who access the Manager's digital channels or physical premises, including through access control and monitoring systems. This definition also covers former clients, former Personnel and other data subjects whose data remains under processing by reason of a legal or regulatory obligation or of the regular exercise of rights. Data relating to legal entities does not constitute Personal Data, except where it allows a natural person to be identified, directly or indirectly.
Controller[13]	The natural person or legal entity, governed by public or private law, **responsible for the decisions concerning the processing of Personal Data**. In the context of the Manager, Tera acts as Controller of the data collected directly from its Clients, Personnel and Service Providers, since it determines the purpose and the means of such processing, including, without limitation, for purposes of registration, *Know*

[11] As defined in art. 5, IV, of the LGPD.
[12] As defined in article 5, V, of the LGPD.
[13] As defined in art. 5, VI, of the LGPD.

	Your Client, Know Your Partner and Know Your Employee procedures, contract performance and compliance with legal and regulatory obligations before the CVM and ANBIMA.
Processor[14]	The natural person or legal entity, governed by public or private law, **that carries out the processing of Personal Data on behalf of the Controller**. Tera's role as Processor is exceptional. In its relationships with the fiduciary administrator, the distributor, the custodian and other market participants, Tera and such participants act, as a rule, as independent Controllers, each determining the purposes of the Processing necessary to comply with its own regulatory obligations.
Data Protection Officer[15]	A member of the Manager's Personnel: Alan Lima (alan.lima@teracapital.com.br or dpo@teracapital.com.br). The Data Protection Officer is responsible for accepting complaints and communications from Data Subjects, providing clarifications and taking appropriate measures, receiving communications from the ANPD, guiding Personnel and performing the other duties set out in article 41 of the LGPD. The identity and contact details of the Data Protection Officer are publicly disclosed on the Manager's website.
Processing Agents[16]	An expression designating, jointly, the Controller and the Processor. In the context of the Manager, Tera itself qualifies as a Processing Agent (in the situations described above), as do the contracted third parties that have access to Personal Data in the exercise of their activities (e.g., fiduciary administrator, custodian, distributor, specialized consultant and other service providers), and the Manager must contractually formalize the roles, responsibilities and legal bases applicable to each relationship.
Compliance Department[17]	The department responsible for: (a) mapping and processing the Personal Data that Tera receives in its interactions with Personal Data Subjects; (b) ensuring that the sharing of Personal Data with third parties is carried out in accordance with the rules established in the LGPD and in this Policy; (c) prohibiting the sharing of Personal Data in cases where compliance with the rules established in the LGPD and in this Policy is not possible; and (d) periodically updating this Policy.
Processing[18]	Any operation carried out with Personal Data, such as those relating to collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction.

[14] As defined in art. 5, VII, of the LGPD.
[15] As defined in art. 5, VIII, of the LGPD.
[16] As defined in art. 5, IX, of the LGPD.
[17] As defined in the Compliance Manual.
[18] As defined in art. 5, X, of the LGPD

Personnel	Partners, officers, employees, interns, apprentices and individual service providers acting on behalf of the Manager, regardless of the nature of the relationship, as defined in the Compliance Manual.
Shared Use of Data	The communication, dissemination, international transfer, interconnection or shared processing of Personal Data by two or more Processing Agents, subject to item 2.5 of this Policy.
International Transfer of Data	The transfer of Personal Data to a foreign country or to an international organization of which Brazil is a member, subject to the situations set out in article 33 of the LGPD and to RANPD 19, as provided in Chapter 5 of this Policy.
Security Incident	An adverse event, confirmed or suspected, related to a security breach that results in unauthorized access, destruction, loss, alteration, leakage or any form of inappropriate Processing of Personal Data, even if accidental, as provided in Chapter 4 of this Policy.
ANPD	The Brazilian National Data Protection Authority, a federal public administration body responsible for safeguarding the protection of Personal Data and for supervising and imposing sanctions in the event of non-compliance with the LGPD.

2. Processing of Personal Data by Tera

2.1. Principles Applied to the Processing of Personal Data

All Processing of Personal Data carried out by Tera shall observe good faith and the principles set out in article 6 of the LGPD, applied as follows:

(i) **Purpose**: each Processing activity has a specific purpose, and any subsequent use incompatible with that purpose is prohibited;

(ii) **Suitability**: the data processed must be compatible with the purpose informed to the Data Subject and with the context in which it was obtained;

(iii) **Necessity:** only the data necessary for the provision of Tera's services and for compliance with applicable legislation and regulation is collected;

(iv) **Free Access**: the Data Subject is granted facilitated and free-of-charge consultation regarding the Processing of their data, as provided in Chapter 3 of this Policy and in the LGPD;

(v) **Quality of Personal Data**: registration data is kept accurate and up to date, with a frequency compatible with the applicable regulation;

(vi) **Transparency:** the information on the Processing is clear and accessible, subject to trade and industrial secrets and to the confidentiality required by capital markets regulation;

(vii) **Security:** the technical and administrative measures established in Tera's internal policies apply;

(viii) **Prevention**: Tera acts preventively, and not merely in response to incidents, pursuant to Chapter 4;

(ix) **Non-Discrimination**: Processing for unlawful or abusive discriminatory purposes is prohibited;

(x) **Accountability:** Tera maintains documentation capable of evidencing the adoption and effectiveness of the measures set out in this Policy.

2.2. Sources of Personal Data

The Personal Data processed by Tera is obtained from the following sources:

(i) **Directly from the Data Subject**: upon completion of the registration form, the investor profile analysis questionnaire, tax forms (FATCA and CRS), contracts and other pre- and post-contracting documents, as well as in the course of the relationship;

(ii) **Service Providers and Other Market Participants:** fiduciary administrator, custodian, registrar, distributor, specialized consultant and other participants in the transactions and vehicles under management, within the scope of their respective regulatory and contractual duties;

(iii) **Public Sources and Third-Party Databases**: domestic and international restrictive lists, politically exposed persons databases, adverse media, official publications, courts, commercial registries and contracted reputational due diligence tools;

(iv) **Generated Internally by Tera**: service records, institutional correspondence, system access *logs* and, where applicable, recordings and transcriptions of meetings, pursuant to item 2.7;

(v) **Received Incidentally or Unsolicited**: pursuant to item 2.2.1 below.

2.2.1. Personal Data Received Incidentally or Unsolicited

If Tera, through its Personnel, receives Personal Data incidentally or unsolicited (i.e., copied on an electronic message containing personal information of third parties), such data shall not be used for any purpose of the Manager, shall not be incorporated into its databases or passed on to third parties, and must remain restricted to the context in which it was received.

Communication to the Data Protection Officer is required only where the receipt: (i) involves Sensitive Personal Data, as provided in item 2.6; (ii) covers a material volume of Data Subjects; (iii) results in the incorporation of the data into a system or database of the Manager; or (iv) indicates the occurrence of a Security Incident, whether its own or that of a third party, in which case Chapter 4 applies.

2.3. Purposes of Processing and Legal Bases for the Processing of Personal Data

Tera processes Personal Data for the purposes indicated in the table below, based on the existing legal bases. The table below fulfills the requirement set out in article 9, item V, of the ANBIMA Rules and Procedures on Basic Duties, which provides for the obligation to specify the privacy controls applicable to Personal Data to which participating institutions have access:

#	Purpose	Data Subjects	Legal basis	Retention	Responsible
1	Registration, identification, qualification and registration updates of Clients, including Know Your Client (KYC) procedures	Clients and representatives	Compliance with a legal or regulatory obligation (art. 7, II, LGPD); RCVM 50 and RCVM 21	Min. 5 (five) years from registration or from the last update (RCVM 50, art. 26, § 2)	Compliance
2	Anti-money laundering and counter-terrorism financing due diligence: restrictive list searches, politically exposed person screening, adverse media,	Clients, Personnel, Service Providers	Art. 7, II, LGPD; Law No. 9,613/1998; Law No. 13,810/2019; RCVM 50	Min. 5 (five) years, extendable by determination of the CVM (RCVM 50, art. 26)	Compliance

#	Purpose	Data Subjects	Legal basis	Retention	Responsible
	transaction monitoring and reports to COAF				
3	Investor profile analysis	Clients	Art. 7, II, LGPD for regulated services	Min. 5 (five) years (RCVM 21, art. 34)	Portfolio Management and Compliance
4	Performance of discretionary portfolio management, wealth management and investment consolidation agreements	Clients	Performance of a contract (art. 7, V, LGPD)	Term of the agreement + 5 (five) years	Compliance and Portfolio Management
5	Management of investment funds and vehicles and relationship with unitholders, including support for unitholders' meetings and provision of information	Clients	Art. 7, II and V, LGPD; RCVM 175; RCVM 21	Min. 5 (five) years (RCVM 175, art. 130; RCVM 21, art. 34)	Compliance and Portfolio Management
6	Provision of information to regulators and self-regulatory bodies (CVM, ANBIMA, BACEN, COAF) and to tax authorities, including within the scope of CRS and FATCA	Clients, Personnel and Service Providers	Art. 7, II, LGPD	Min. 5 (five) years (RCVM 21, art. 34)	Compliance
7	Regular exercise of Tera's rights in judicial, administrative or arbitration proceedings and response to inspections and requests from competent authorities	All	Regular exercise of rights (art. 7, VI, LGPD)	Until the final and unappealable decision	Legal and Compliance
8	Response to requests from Data Subjects in the exercise of the rights set out in article 18 of the LGPD	All	Art. 7, II, 18 and 19, LGPD	5 (five) years from the closing of the request	Compliance and Data Protection Officer
9	Information and cyber security, access control to systems and environments, monitoring of corporate resources and fraud prevention	Clients, Personnel and third parties with access	Legitimate interest (art. 7, IX, LGPD)	12 (twelve) months for *logs*	Technology and Compliance
10	Recruitment and selection of Personnel	Personnel and candidates	Preliminary procedures (art. 7, V, LGPD); talent pool based on legitimate interest (art. 7, IX, LGPD)	12 (twelve) months after the process.	Human Resources and Compliance
11	Reputational due diligence on Personnel, candidates, Service Providers and counterparties (KYE/KYP)	Personnel, candidates, Service Providers	Art. 7, II, LGPD where required by regulation; beyond that, legitimate interest (art. 7, IX, LGPD)	Min. 5 (five) years (RCVM 21, art. 34)	Compliance
12	Recording and transcription of meetings and use of support tools based on artificial intelligence	Clients, Personnel, Service	Legitimate interest (art. 7, IX, LGPD); Consent where required under	12 (twelve) months	Data Protection Officer and

#	Purpose	Data Subjects	Legal basis	Retention	Responsible
		Providers	item 2.4.5		Technology
13	Compliance with the Manager's internal policies and manuals, investigation of breaches and response to security incidents	All	Art. 7, II and IX, LGPD	Min. 5 (five) years	Compliance and Data Protection Officer
14	Administration of the employment relationship: payroll, benefits, working hours, occupational health and safety and other labor and social security obligations	Personnel and their dependents	Performance of a contract (art. 7, V, LGPD) and legal or regulatory obligation (art. 7, II); health data pursuant to art. 11, II, "a"	Periods set out in labor and social security legislation, subject to a minimum of 5 (five) years after termination of the relationship	Human Resources and Compliance
15	Physical access control to the Manager's premises and monitoring by video surveillance system	Personnel, Service Providers and visitors	Legitimate interest (art. 7, IX, LGPD); specific Consent for biometric data (art. 11, I), as provided in item 2.6	Up to 90 (ninety) days for images and access records	Technology and Compliance
16	Structuring and monitoring of wealth and succession planning solutions, including through vehicles incorporated abroad	Clients, family group members and beneficiaries	Performance of a contract (art. 7, V, LGPD); as regards family group members and beneficiaries, legitimate interest (art. 7, IX), subject to a balancing test	Term of the agreement + 5 (five) years	Portfolio Management and Compliance
17	Institutional communications, distribution of materials and relationship activities unrelated to the performance of the agreements	Clients and prospective Clients	Legitimate interest (art. 7, IX, LGPD), with the right to object assured; Consent where required under item 2.4.5	Until the Data Subject objects	Portfolio Management and Compliance

2.3.1. Legal Bases Not Applicable to Tera's Activities

Tera declares that it does not carry out any Processing of Personal Data on the basis of the following situations set out in article 7 of the LGPD, as they bear no relation to its activities:

(i) processing and shared use by the public administration for the implementation of public policies;
(ii) conducting studies by a research body;
(iii) protection of health in procedures carried out by health professionals, health services or sanitary authorities;
(iv) credit protection.

The situation set out in item VII of article 7 (protection of the life or physical safety of the Data Subject or of a third party) does not constitute an ordinary legal basis for any of Tera's activities, and may be invoked only in a specific emergency situation, with immediate recording by the Data Protection Officer.

2.4. Specific Requirements by Legal Basis

2.4.1. Compliance with a Legal and/or Regulatory Obligation (art. 7, II, LGPD)

This basis applies whenever the Processing is necessary to comply with an obligation established in a law, decree, resolution, instruction, official letter, self-regulatory ruling or other normative act applicable to Tera's activities, including the obligations relating to registration and registration updates, anti-money laundering and counter-terrorism financing, investor profile verification, retention of documents and records, provision of information to regulators, self-regulatory bodies and tax authorities, including within the scope of CRS and FATCA, and response to requests from competent authorities.

2.4.2. Performance of a Contract and Preliminary Procedures (Art. 7, V, LGPD)

This basis applies where the Processing is necessary for the performance of a contract to which the Data Subject is a party or for the adoption of preliminary procedures related to a contract, at the request of the Data Subject (i.e., discretionary portfolio management, wealth management and financial and non-financial asset consolidation agreements, as well as proposals, simulations and *onboarding* steps requested by the Data Subject prior to contracting).

Obligations arising from the regulation or self-regulation applicable to Tera's activities do not fall under this legal basis, even if performed in the context of a contract. Such obligations are based on item 2.4.1 above. This distinction is relevant because, once the contract has ended, the regulatory retention duty remains in force.

2.4.3. Regular Exercise of Rights (art. 7, VI, LGPD)

This basis applies to Processing necessary for the defense of Tera's interests in judicial, administrative or arbitration proceedings (Law No. 9,307/1996), as well as to responding to inspections and requests from competent authorities. The Processing is limited to the data relevant to the subject matter of the dispute or request and ceases upon the final and unappealable decision or the closing of the proceeding, subject to the applicable statutes of limitation and retention periods.

2.4.4. Legitimate Interest (arts. 7, IX, and 10, LGPD)

Processing based on the legitimate interest of Tera or of a third party requires special attention, so as to ensure a balance between (a) the legitimate interest invoked; and (b) the protection of the rights, fundamental freedoms and legitimate expectations of the Data Subject. In such cases, only the Personal Data strictly necessary for the intended purpose may be processed.

Before the commencement of any Processing based on legitimate interest, the Data Protection Officer, with the support of the Compliance Department, shall prepare and file a balancing test (also referred to as a proportionality test or legitimate interest assessment), addressing, at a minimum:

(i) **Legitimacy of the interest**: the purpose must be legitimate, specific and compatible with Tera's activities, and may not be prohibited by law nor based on a merely future or abstract scenario;

(ii) **Necessity**: it must be demonstrated that the purpose cannot be achieved with less data, and whether another legal basis is more appropriate must be assessed;

(iii) **Balancing**: the impacts on the rights and legitimate expectations of the Data Subject must be analyzed, verifying whether the interest invoked prevails;

(iv) **Safeguards**: mitigation measures must be adopted, such as prior transparency, limitation of

access, minimization, pseudonymization or anonymization and, where applicable, the possibility of objection by the Data Subject, measures which are not to be confused with obtaining Consent.

The recording of operations based on legitimate interest is mandatory, pursuant to article 37 of the LGPD, and Tera may be required by the ANPD to submit a personal data protection impact report, pursuant to article 10, § 3, of the LGPD.

2.4.5. Consent (arts. 7, I, and 8, LGPD)

Consent is a residual and exceptional legal basis in the context of Tera. Reliance on it must be avoided where another legal basis applies, in particular in the cases of compliance with a legal or regulatory obligation and of performance of a contract.

Where Consent is the appropriate legal basis, it must cumulatively meet the following validity requirements:

(i) **Informed**: the Data Subject must be informed in advance of the purpose of the Processing, the data involved, the intended sharing and their rights;

(ii) **Free**: the Data Subject must have effective decision-making power; where possible, the authorization will be broken down by purpose. Where certain information is essential to the provision of the service, this fact will be stated prominently;

(iii) **Unequivocal**: any form of inducement, manipulation or hasty obtaining of the statement is prohibited;

(iv) **Specific**: Consent refers to specific purposes and to specified data or categories of data, and generic authorizations are null and void;

(v) **Prominent**: where collected in writing, Consent shall be set out in a separate instrument or in a clause highlighted from the other contractual clauses, and its diffuse insertion into the body of the services agreement is prohibited.

The burden of evidencing that Consent was duly obtained lies with Tera. The Data Subject may revoke it at any time, by express statement sent to the Data Protection Officer's channel, by means of a free-of-charge and facilitated procedure, and the Processing carried out under the prior Consent up to the revocation remains ratified. The revocation does not affect Processing based on another legal basis, in particular the obligations to retain data and to provide information to regulators.

If there is a change of purpose incompatible with the original Consent, the Data Subject will be informed in advance and may revoke it if they disagree.

In the context of Tera, Consent will be used, in particular: (i) in the Processing of Sensitive Personal Data not covered by the situations set out in article 11, item II, of the LGPD; (ii) in the Processing of data of children and adolescents, in which case it will be collected specifically and prominently from at least one parent or legal guardian, pursuant to article 14, § 1, of the LGPD; and (iii) for ancillary purposes not necessary to the provision of the services, such as institutional communications and the distribution of materials.

2.5. Shared Use of Data, Processors and Third Parties

The sharing of Personal Data is a form of Processing and, as such, requires its own specific purpose and legal basis, which will always be the same as those of the Processing that justifies it, as recorded in the table in item 2.3 above.

Tera shares Personal Data, to the extent necessary, with:

Third party	Purpose	Role
Fiduciary administrator, custodian, registrar and asset and liability controller	Operation of the funds and vehicles under management and of the discretionary managed portfolios	Independent Controller as regards its regulatory duties
Distributor	Distribution of units and relationship with the investor	Independent Controller as regards its regulatory duties
Specialized consultant and other providers engaged in the interest of the portfolios	Performance of the contracted activities	Processor or independent Controller, depending on the contract
Outsourced human resources and payroll provider	Administration of the employment relationship	Processor
Providers of systems, storage and cloud computing, including recording and transcription tools	Support to the Manager's activities	Processor
Auditors, legal advisors and external consultants	Audit, defense of rights and advisory services	Processor or independent Controller, as the case may be
CVM, ANBIMA, BACEN, COAF, the Brazilian Federal Revenue Service and other authorities	Compliance with a legal or regulatory obligation and response to requests	Legal recipient — does not constitute discretionary sharing

The conditions for sharing are:

(i) execution of a contractual instrument containing personal data protection clauses, defining the role of each party, the authorized purposes and other applicable conditions;
(ii) prior due diligence on the third party's ability to comply with this Policy and with data protection legislation, in accordance with Tera's third-party engagement rules; and
(iii) compliance with Chapter 5 of this Policy, where there is an International Transfer of Data.

Any circulation of Personal Data between Tera and other entities of the same economic group constitutes shared use of data and, as such, requires a specific purpose, its own legal basis and information to the Data Subject, and is not authorized by the mere fact of belonging to the same economic group.

2.6. Sensitive Personal Data

As a rule, Tera does not collect or request Sensitive Personal Data from Clients, their representatives or family group members.

The Processing of Sensitive Personal Data by Tera is restricted, as a rule, to the following situations, subject to article 11 of the LGPD:

(i) Health data of Personnel strictly necessary for the administration of benefits and for compliance with labor, social security and occupational health and safety obligations, based on article 11, item II, paragraph "a", of the LGPD;
(ii) Sensitive data indispensable to the regular exercise of rights in judicial, administrative or arbitration proceedings, based on article 11, item II, paragraph "d", of the LGPD; and
(iii) Facial biometric data of Personnel, for the exclusive purpose of controlling access to the Manager's premises, subject to specific and prominent Consent from the member of Personnel (article 11, item I, of the LGPD), with a non-biometric access alternative assured in any event,

without prejudice to any member of Personnel who does not consent.

Exceptionally, within the scope of the provision of wealth and succession planning services, the Manager may receive Sensitive Personal Data of Clients, of members of the Client's family group and of beneficiaries, in which case the Processing shall observe article 11 of the LGPD and the provisions of this item.

If Tera, through its Personnel, receives Personal Data incidentally or unsolicited (i.e., a copy on an electronic message containing personal information of third parties), such data shall not be used for any purpose of the Manager, shall not be incorporated into its databases or passed on to third parties, and must remain restricted to the context in which it was received.

Communication to the Data Protection Officer is required only where the incidental receipt of Sensitive Personal Data: (i) covers a material volume of Data Subjects; (ii) results in the incorporation of the data into a system or database of the Manager; or (iii) indicates the occurrence of a Security Incident, whether its own or that of a third party, in which case Chapter 4 applies.

The status of politically exposed person (PEP), processed for anti-money laundering purposes, does not constitute Sensitive Personal Data within the meaning of article 5, item II, of the LGPD. Even so, given its potential to reveal information of a political nature, Tera processes such data with restricted access and exclusively for the regulatory purpose that justifies it.

2.7. Recording of Meetings, Transcription and Artificial Intelligence Tools

Tera may record and transcribe meetings and use support tools based on artificial intelligence in the processing of communications, documents and records containing Personal Data, exclusively by means of tools previously approved by the Compliance Department and by the department responsible for information technology and cybersecurity, and subject to the rules set out in this item.

Where the recording involves a meeting with a Client and there is no legal basis of performance of a contract or of compliance with a regulatory obligation supporting it, the Data Subject's Consent will be obtained as provided in item 2.4.5, with the right to object at any time.

It is prohibited to enter Personal Data, Sensitive Personal Data or confidential information of Clients, of Personnel or of the portfolios under management into publicly available artificial intelligence tools, into personal accounts or into tools not approved by the Manager, even for purposes of summarizing, translating, reviewing or analyzing.

2.8. Retention and Deletion of Personal Data

Processing ends when the purpose has been achieved, when the data is no longer necessary or relevant to the purpose, at the end of the Processing period, upon communication from the Data Subject or by determination of the ANPD, pursuant to article 15 of the LGPD.

Once the Processing has ended, the Personal Data will be deleted, with retention being authorized, pursuant to article 16 of the LGPD, for: (a) compliance with a legal or regulatory obligation by Tera; (b) transfer to a third party, subject to the requirements of the LGPD; or (c) exclusive use by Tera, with access by third parties prohibited and provided that the data is anonymized.

The deletion of Personal Data that is the subject of ongoing litigation, administrative proceedings, inspection or an authority's request is prohibited, even if the retention period has expired, until the definitive closing of the proceeding.

Deletion will be carried out by a method that prevents the recovery of the information, with a record of the operation, and will cover the copies existing in backup environments, to the extent permitted by the technical limits of the tools used.

2.9. Record of Processing Operations and Impact Report

Tera maintains a record of the Personal Data Processing operations it carries out, pursuant to article 37 of the LGPD, in particular those based on legitimate interest. The record is prepared and maintained by the Compliance Department, with the support of the departments involved.

The record of processing operations is reviewed whenever there is a material change in activities, contracts, systems or suppliers, and must remain consistent with the tables in items 2.3 and 2.4 above.

Tera will prepare a personal data protection impact report, containing a description of the types of data collected, the methodology used for collection and for ensuring security, and an analysis of the measures, safeguards and risk mitigation mechanisms adopted, in the following situations: (a) when so determined by the ANPD, pursuant to article 38 of the LGPD; (b) when the Processing is based on legitimate interest and is requested by the ANPD, pursuant to article 10, § 3; and (c) by resolution of the Data Protection Officer, where Processing is carried out for a new purpose not indicated in the table in item 2.3.

2.10. Security of Processing

Tera adopts technical and administrative security measures capable of protecting Personal Data from unauthorized access and from accidental or unlawful destruction, loss, alteration, communication or any form of inappropriate Processing, pursuant to article 46 of the LGPD. The specific measures, access controls, periodic testing and confidentiality rules are set out in the Manager's information security policy and confidentiality manual, as required by articles 24 and 28 of RCVM 21 and by articles 9 to 12 of the ANBIMA Rules and Procedures on Basic Duties.

Security incidents involving Personal Data follow the workflow set out in Chapter 4 of this Policy.

3. Rights of Personal Data Subjects

The Subjects of Personal Data have several rights in relation to Personal Data and Sensitive Personal Data. The following rights have been mapped:

3.1. Confirmation of Existence of and Access to Personal Data: The Personal Data Subject may request from the Manager confirmation of the existence of, and/or access to, their Personal Data. Confirmation of existence or access will be provided immediately, in simplified format, or, if so requested by the Data Subject, by means of a clear and complete statement, within the period set out in item 3.10, indicating the origin of the data, the absence of records, the criteria used and the purpose of the Processing, pursuant to article 19, items I and II, of the LGPD.

3.2. Correction of Personal Data: The Personal Data Subject may request Tera to correct incomplete, inaccurate or outdated data.

3.3. Anonymization, Blocking or Deletion of Personal Data: The Personal Data Subject may request the anonymization, blocking or deletion of unnecessary or excessive data, or of data processed in breach of the

LGPD. Compliance with such request is subject to the retention situations set out in article 16 of the LGPD and does not cover Personal Data whose retention is required by a legal or regulatory obligation, in particular for the periods indicated in the table in item 2.3, nor data necessary for the regular exercise of rights. In such cases, Tera will inform the Data Subject of the factual and legal reasons preventing the adoption of the measure, pursuant to article 18, § 4, of the LGPD.

For the purposes of this Policy, unnecessary and excessive data means data that is no longer useful for the specific Processing purpose previously intended.

3.4. Portability of Personal Data: The Data Subject may request the portability of the data to another service or product provider, upon express formal request to the Manager, in accordance with ANPD regulation and the LGPD. In such case, Tera's trade and industrial secrets must be kept confidential.

It should be noted that data that has been anonymized by the Manager will not be included in the portability.

Finally, it is important to point out that, even where portability is carried out, the Manager must retain the Personal Data for purposes of compliance with the applicable regulation in force, in accordance with the legal or contractual period(s).

3.5. Deletion of Personal Data Processed on the Basis of Consent: Considering that Consent may be revoked at any time by means of a formal and express statement from the Data Subject to the Manager, through a free-of-charge and facilitated procedure, the deletion of the Personal Data must occur within a reasonable period after receipt of the request.

However, the Manager is authorized to retain the Personal Data in the following situations:

(i) Personal Data obtained for compliance with a legal or regulatory obligation by the Manager;

(ii) For transfer to a third party, such as for purposes of International Transfer of Data and Shared Use of Data, provided that the data processing requirements set out in the LGPD are observed; or

(iii) For the exclusive use of the Manager, with access by third parties prohibited and provided that the data is anonymized.

3.6. Information on the Sharing of Personal Data: The Personal Data Subject has the right to be clearly informed about the sharing of their data with third parties. The circulation of Personal Data between entities of the same economic group, even if under different corporate taxpayer registrations, constitutes Shared Use of Data and requires a specific purpose, its own legal basis and information to the Data Subject.

3.7. Objection to Processing: The Data Subject may object to Processing carried out on the basis of one of the situations in which Consent is waived, in the event of non-compliance with the LGPD, pursuant to

article 18, § 2. The Manager further assures the possibility of objecting to Processing based on legitimate interest, as provided in item 2.4.4.

3.8. Review of Automated Decisions: The Data Subject may request the review of decisions taken solely on the basis of automated Processing of their Personal Data that affect their interests, pursuant to article 20 of the LGPD. As of the date of this Policy, the Manager does not adopt solely automated decisions with such effects; should it come to adopt them, it will inform the Data Subjects in advance, together with the criteria used, subject to item 2.7.

3.9. Information on the Refusal of Consent and Petition to the ANPD: The Data Subject has the right to be informed of the possibility of not providing Consent and of the consequences of such refusal, as well as of the right to petition against the Manager before the ANPD, pursuant to article 18, items VI and VII, of the LGPD.

3.10. Form of Request and Response Deadline: Should the Data Subject wish to exercise any of the rights set out in items 3.1 to 3.9 above, they must send the relevant request to the Manager by e-mail to dpo@teracapital.com.br. The Data Protection Officer will confirm the identity of the requesting party before providing any information and, in the case of a request submitted by a legal representative, attorney-in-fact, heir or estate administrator, will require documentary evidence of their powers.

Tera will respond to each request within a maximum of 15 (fifteen) days from receipt, in accordance with the period set out in article 19, item II, of the LGPD for the statement of confirmation and access, which the Manager has adopted, for standardization purposes, for the other rights as well. Where it is not possible to comply with the request, Tera will inform the Data Subject, within the same period, of the factual or legal reasons preventing the immediate adoption of the measure.

4. Response to Security Incidents

4.1. Purpose

This section establishes the procedure and the applicable deadline for the notification of security incidents involving Personal Data processed by the Manager, in accordance with the Brazilian General Personal Data Protection Law and with the regulation issued by the ANPD.

4.2. Applicable Deadline

Pursuant to the LGPD and to RANPD 15, security incidents that may result in relevant risk or damage to Personal Data Subjects must be notified to the ANPD and to the affected Data Subjects within 3 (three) business days, counted from the date on which the Manager becomes aware of the incident.

The notification to the ANPD is submitted through the electronic form made available by the Authority. Where it is not possible to gather all the required information within the deadline, the Manager will submit the notification with the information available, justifying the absence of the remainder, and will supplement it within up to 20 (twenty) business days, pursuant to RANPD 15.

Where Tera acts as Processor, it will notify the incident to the Controller immediately after becoming aware of it, and the Controller shall be responsible for notifying the ANPD and the Data Subjects. The agreements entered into with the Manager's Processors must provide for the immediate notification of incidents to Tera.

4.3. Internal Incident Response Workflow

4.3.1 Overview

The Manager adopts a workflow structured in 6 (six) stages for the identification, assessment, containment and, where applicable, notification of security incidents involving Personal Data of Data Subjects, as detailed below.

4.3.2 Stages of the Workflow

(a) **Detection and Recording:** Any member of Personnel who identifies or suspects the occurrence of a security incident (such as a data leak, improper access, loss or theft of a device, or sending an e-mail to an incorrect recipient) must report the fact immediately to the Data Protection Officer, through the single institutional channel made available for that purpose (dpo@teracapital.com.br).

Accurate recording of the time of detection is a critical element of the process, since the legal notification deadline referred to in Section 4.2 is counted from the moment Tera becomes aware of the incident, and not from its occurrence.

(b) **Triage and Risk Classification:** The Data Protection Officer is responsible for assessing the nature of the reported incident and classifying the associated risk level (low, medium or high) within up to 24 (twenty-four) hours from receipt of the report, taking into account, among others, the following criteria:

(i) Type of Personal Data involved;
(ii) Volume and category of Data Subjects potentially affected;
(iii) Whether the information was in fact exposed to third parties; and
(iv) Potential for damage to the data subjects.

The risk classification determines whether the incident must be escalated to the Technology Department[19], the Manager's technology support and cybersecurity provider, internal or external legal counsel and/or any business area involved in the incident.

[19] As defined in the Manager's Compliance Manual.

(c) **Containment:** Once the incident has been identified, the measures necessary for its containment must be adopted immediately, such as revocation of access, isolation of affected systems, recall of improperly sent communications and notification to the supplier or processor involved. At this stage, the priority is to stop the exposure of the data, even if the investigation of the root cause of the incident is concluded subsequently;

(d) **Analysis and Decision on Notification:** Once containment has been completed, the root cause of the incident is investigated, the actual scope of the impact is determined (number of Data Subjects affected and categories of data compromised) and the technical security measures already in place are verified. On the basis of these elements, the Data Protection Officer is responsible for deciding whether the incident constitutes relevant risk or damage to the Data Subjects, a criterion that determines whether notification to the ANPD and to the affected Data Subjects is mandatory, in accordance with the communication templates set out in Annex I to this Policy;

(e) **Notification:** Where notification is found to be mandatory, it must be made to the following interested parties:

(i) **ANPD**: a notification containing the nature of the Personal Data affected, the Data Subjects involved, the technical and security measures used to protect the data, the risks related to the incident and the measures that have been or will be adopted to reverse or mitigate its effects; and

(ii) **Affected Data Subjects**: a communication in clear and accessible language, describing what occurred, which data was impacted, the measures taken by Tera and the measures that the Data Subject may adopt to protect themselves; and

(iii) **The fiduciary administrator, the distributor and other affected Processing Agents, as well as the CVM and ANBIMA, where the incident affects data or systems related to the vehicles under management or where there is a reporting duty arising from regulation, self-regulation or the agreements entered into.**

(f) **Remediation and Historical Record:** After containing the incident, Tera must review the control that gave rise to the failure and update the relevant policies, processes and/or systems in order to prevent its recurrence. All incidents, including those not notified to the ANPD, must be fully documented and retained for a minimum period of 5 (five) years, so as to evidence compliance with the accountability principle in any supervisory proceeding.

5. International Transfer Of Data

The International Transfer of Data will only be carried out where one of the situations set out in article 33 of the LGPD is present and in compliance with the International Data Transfer Regulation (RANPD 19). A transfer based on an adequacy decision depends on formal recognition, by the ANPD, of the country or international organization of destination, and it is not for the Manager to assess independently the equivalence of foreign legislation. As of the date of this Policy, the ANPD has recognized only the European Union as adequate, by means of CD/ANPD Resolution No. 32/2026.[20]

[20] As defined in art. 5, XV, of the LGPD.

The transfer may take place where (i) cooperation between public intelligence bodies of different countries is necessary for purposes of criminal investigation and prosecution; (ii) the transfer is necessary for compliance with a legal or regulatory determination by the Controller; (iii) it is necessary for the performance of a contract or of preliminary procedures related to a contract; (iv) it is for the regular exercise of rights in judicial, administrative or arbitration proceedings; or (v) it is for the implementation of public policies or legal requirements of the public service.

In addition, the International Transfer of Data may also occur where the Controller offers and evidences guarantees of compliance with the principles, the rights of the Data Subject and the data protection regime set out in the LGPD, in the form of:

(a) specific contractual clauses for a given transfer;
(b) standard contractual clauses;
(c) global corporate rules; and
(d) seals, certificates and codes of conduct duly issued.
(e) A transfer authorized by specific and prominent Consent of the Data Subject, preceded by information on the international nature of the operation and clearly distinguished from other purposes (article 33, item VIII, of the LGPD), constitutes an autonomous legal situation and not a form of guarantee.

Accordingly, the Manager has the duty to ensure compliance with these principles by means of contractual clauses, certificates and other recognized evidence.
The standard contractual clauses approved by the ANPD must be adopted in full, without any change to their content, and only adjustments to the fields expressly intended for the particulars of the transaction are permitted, under penalty of invalidity; they do not require prior approval by the Authority. Specific contractual clauses and global corporate rules, by contrast, require prior approval by the ANPD.
In the context of the Manager, International Transfers of Data are carried out, among other situations, to: (i) investment vehicles and structures incorporated abroad, including trusts and private investment companies, and their respective trustees, administrators and agents; (ii) foreign financial institutions, custodians and brokers; (iii) foreign legal and tax advisors; (iv) providers of systems, cloud storage and recording, transcription and artificial intelligence tools whose processing takes place outside Brazilian territory; and (v) foreign tax authorities, through the Special Department of Federal Revenue of Brazil, within the scope of CRS and FATCA.

By way of example, mention may be made of the request for identification of the *Ultimate Beneficial Ownership* (UBO) by a foreign public authority, as well as the completion of forms within the scope of the CRS (*Common Reporting Standard*) and of the W-8 (FATCA). In all such cases, the International Transfer of Data would be authorized by the LGPD itself, pursuant to its art. 33, item IX.

6. Penalties

The LGPD provides that sanctions will be applied following an administrative proceeding affording the opportunity for a full defense, on a gradual, isolated or cumulative basis, in accordance with the particulars of the specific case and taking into account, among others, the following parameters and criteria:

(a) the seriousness and nature of the violations and of the personal rights affected;
(b) the good faith of the offender;
(c) the degree of the damage;
(d) the cooperation of the offender;
(e) the existence of internal mechanisms and procedures capable of minimizing the damage, aimed at the secure and appropriate processing of data; and
(f) the adoption of a best practices and governance policy.

The penalties applicable to Processing Agents that fail to comply with the provisions of the LGPD may be the following:

(i) a warning, indicating a deadline for the adoption of corrective measures;
(ii) a simple fine of up to 2% (two percent) of the revenues of the private legal entity, group or conglomerate in Brazil in its last financial year, excluding taxes and limited, in total, to BRL 50,000,000.00 (fifty million reais) per violation;
(iii) a daily fine limited, in total, to BRL 50,000,000.00 (fifty million reais) per violation;
(iv) public disclosure of the violation once its occurrence has been duly ascertained and confirmed;
(v) blocking of the Personal Data to which the violation relates until its regularization;
(vi) deletion of the Personal Data to which the violation relates;
(vii) partial suspension of the operation of the Database to which the violation relates for a maximum period of 6 (six) months, extendable for an equal period, until the processing activity is regularized by the Controller; or
(viii) suspension of the exercise of the activity of processing the Personal Data to which the violation relates for a maximum period of 6 (six) months, extendable for an equal period.
(ix) The administrative sanctions set out in this Chapter do not exclude the Manager's civil liability towards the Data Subjects, pursuant to articles 42 to 45 of the LGPD, nor the sanctions applicable by the CVM and by ANBIMA as a result of non-compliance with regulation and self-regulation.
(x) Non-compliance with this Policy by a member of Personnel subjects them to the disciplinary measures set out in the Manager's internal policies, proportionate to the seriousness of the conduct, without prejudice to any applicable civil and criminal liability.

6.1. Governance, Approval, Training and Review

This Policy is approved by the Manager's board of officers, and the Compliance Department, with the support of the Data Protection Officer, is responsible for its preparation, updating and internal disclosure.

The Policy will be reviewed whenever there is a material legislative or regulatory change, or a significant change in the Manager's activities, systems or service providers, and, in any event, within a period not exceeding 24 (twenty-four) months, pursuant to article 4, sole paragraph, of the ANBIMA Rules and Procedures on Basic Duties.

Personnel receive training on personal data protection upon hiring and, at a minimum, annually, and the Compliance Department maintains the attendance records.

Personnel execute an acknowledgment of this Policy and a confidentiality undertaking, pursuant to article 12 of the ANBIMA Rules and Procedures on Basic Duties.

7. Annexes

5.1. Communication Templates

7.1.1. Template for Communication to the ANPD

SECURITY INCIDENT NOTIFICATION — LGPD

To the Brazilian National Data Protection Authority (ANPD)

1. IDENTIFICATION OF THE CONTROLLER

Corporate name: Tera Investimentos Ltda.

CNPJ: 30.782.926/0001-47

Address: [full address]

2. IDENTIFICATION OF THE DATA PROTECTION OFFICER (DPO)

Name: [name of the Data Protection Officer]

E-mail: [contact e-mail]

Telephone: [contact telephone number]

3. RELEVANT DATES

Date and time on which the Manager became aware of the incident: [dd/mm/yyyy, hh:mm]

Estimated date and time of occurrence of the incident: [dd/mm/yyyy, hh:mm **or** "under investigation"]

Date of this notification: [dd/mm/yyyy]

4. DESCRIPTION OF THE NATURE OF THE PERSONAL DATA AFFECTED

Categories of data involved: [e.g., name, taxpayer ID, e-mail, registration data / sensitive data, if any]

Estimated volume of records affected: [quantity **or** "under investigation"]

5. INFORMATION ON THE DATA SUBJECTS INVOLVED

Category of data subjects: [**clients / personnel / counterparties / job candidates**]

Estimated number of data subjects affected: [number **or** "under investigation"]

6. TECHNICAL AND SECURITY MEASURES USED

Description of the technical and administrative protection measures in force at the time of the incident: [e.g., encryption, access control, network segmentation, backup], subject to the trade and industrial secrets of the Manager.

7. RISKS RELATED TO THE INCIDENT

Description of the risks and potential damages to Data Subjects arising from the incident: [e.g., risk of fraud, misuse of data, financial exposure].

8. REASON FOR THE DELAY [(if applicable)]

[To be completed only if the notification was not made immediately upon becoming aware of the incident; describe the objective reasons for the delay]

9. MEASURES ADOPTED OR TO BE ADOPTED

Containment measures already implemented: [e.g., revocation of access, isolation of systems, notification to the suppliers involved]

Corrective measures planned to mitigate effects and prevent recurrence: [describe]

10. PERSON RESPONSIBLE FOR THE NOTIFICATION

Name: [name of the Data Protection Officer **or** responsible person]

Signature/position: [Personal Data Protection Officer **or** Tera Investimentos Ltda.]

7.1.2. Template for Communication to Data Subjects

Subject: **Important notice regarding the security of your personal data**

Dear [name of the Data Subject],

We are contacting you to inform you of a security incident that may have affected some of your personal data processed by Tera Investimentos Ltda.

Description of the occurrence:

[Describe in a simple and direct manner what occurred, avoiding technical terms — e.g.: "we identified unauthorized access to one of our systems" **or** "an e-mail containing your data was sent in error to an incorrect recipient"]

When it occurred and when we identified it: The incident occurred on [estimated date or period] and was identified by our team on [date].

Which data was involved:

[List objectively, e.g.: full name, taxpayer ID, e-mail. If sensitive data is involved, state this clearly]

What we have already done:

As soon as we identified the incident, we adopted the following measures:

[e.g.: "we blocked the affected access", "we notified the competent authorities", "we strengthened the security controls of the system involved"].

What we recommend that you do:

[Practical guidance proportionate to the risk, e.g.: "be alert to suspicious messages or calls in your name", "avoid sharing additional information if you are contacted by unidentified third parties", "change your password for access to our portal, as a precaution"]

If you have any questions:

Our Personal Data Protection Officer is available to provide clarifications by e-mail at [e-mail of the Data Protection Officer] or by telephone at [telephone and e-mail of the Data Protection Officer].

We reaffirm our commitment to the protection of your personal data and apologize for any inconvenience caused by this incident.

Sincerely,

Tera Investimentos Ltda.

[Name of the Data Protection Officer]

Personal Data Protection Officer (DPO)

Notes:

- Complete and send the communication to the Data Subjects only after (or simultaneously with) the notification to the ANPD, keeping the two versions consistent as to the facts described.
- Keep a copy of both communications, with the date and time of dispatch, in the incident register maintained by the Data Protection Officer (minimum of 5 years), as already provided for in the internal incident response workflow.
- The notification to the ANPD must be submitted through the electronic form made available by the Authority on its website. This template is intended for the prior organization of the information and for the documentary record of the occurrence.