


<p>PERSONAL DATA PROTECTION POLICY</p> 	<p>SIG_PRO_INC_005</p>
<p>Property iuvity</p> <p>The information in this document is the property of and for internal use by TODO1. The information in this document cannot be disclosed or reproduced outside the company without prior authorization from TODO1.</p>	

Author(s)	Vice-Presidency for Security and Compliance			
CHANGE AND REVIEW HISTORY				
Version/ Review Date	Reviewed by	Approvals	Approval Position	Modification/R eview Description
1.0/ 21-Aug-2020	Ampelio Martin	Information Security Committee	Principal Members Information Security Committee	Document creation for compliance with the ISO/IEC 27001:2013 standard
2.0/ 24-march-2023	Luisa Velasco	Information Security Committee	Principal Members Information Security Committee	Communication channels for personal data requests are defined,

				definition of semi-private data is added, Todo1 is transformed to luvity.

Table of Contents

- 1. PRELIMINARY CONSIDERATIONS.....5
 - 1.1 Document Objective.....5
 - 1.2 Scope.....5
 - 1.3 Reference Documents.....5
 - 1.4 Vocabulary.....5
 - 1.5 Related Documents.....7
- 2. GENERAL PRINCIPLES, POSTULATES and SPECIFIC PRINCIPLES.....9
 - GENERAL PRINCIPLES AND POSTULATES.....9
 - SPECIFIC PRINCIPLES.....9
- 3. TODO1 PERSONAL DATA CONTROLLER AND DATA PROCESSOR.....11
- 4. PERSONAL DATA PROCESSING ACTIVITY LOG.....12
- 5. MAIN SCENARIOS AND SPECIFIC PURPOSES FOR PERSONAL DATA PROCESSING.....22
- 6. DATA SUBJECT AUTHORIZATION AND CONSENT26
 - Means and Manifestations to Grant Authorization.....26
 - Proof of Authorization.....26
- OBLIGATIONS OF THIRD-PARTY VENDORS.....27
- EMPLOYEE OBLIGATIONS.....27
- 7. DATA SUBJECT RIGHTS MANAGEMENT AND ATTENTION PROCEDURES.....29
 - CHANNELS ENABLED FOR DATA SUBJECTS TO EXERCISE THEIR RIGHTS.....34
- 8. ON SPECIAL PROVISIONS FOR PERSONAL DATA PROCESSING AND ACCREDITATION OF “PROACTIVE ACCOUNTABILITY” PRINCIPLES.....35
 - IDENTIFYING AND UPDATING THE PERSONAL INFORMATION CYCLE.....35
 - THIRD-PARTY RELATIONS.....35
 - PRIVACY IMPACT REVIEW.....36
- 9. INFORMATION SECURITY AND PRIVACY RISK MANAGEMENT38

Organizational Measures: 39

Technical Measures: Include the measures and definitions associated with the following aspects:..... 39

10. COMPREHENSIVE CORPORATE PERSONAL DATA PROTECTION PROGRAM..... 41

11. CCTV SYSTEM..... 43

12. FINAL PROVISIONS..... 44

AMENDMENTS TO THE POLICY 44

13. APPLICABILITY 45

Review Timetable 46

14. REGISTRATION CONTROL 47

1. PRELIMINARY CONSIDERATIONS

1.1 Document Objective

The objective of this document is to define general guidelines for the personal data protection implementation, application, monitoring, upkeep, and continuous improvement.

1.2 Scope

TODO1, as Data Controller, acknowledges the importance of the security, privacy, and confidentiality of the personal data of its employees, clients, vendors, partners, commercial partners, and, in general, all its stakeholders whose personal information it processes. Thus, in compliance with constitutional and legal mandates, it submits the following document containing its personal data processing and protection policies for all activities involving personal data processing, subject to regulations, agreements, and treaties that apply in countries where TODO1 has a presence.

1.3 Reference Documents

This document is aligned to ISO/IEC 27001:2013 requirements and makes reference to the following:

- ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary.
- ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.
- ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls.
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- ORGANIC LAW 3/2018 from December 5. Protection of personal data and guarantees for digital rights.
- LSSICE – LAW 34/2002, from July 11, on information society and electronic commerce services.
- ROYAL DECREE 3/2010, from January 8, which regulated the National Security Scheme in the area of Electronic Administration.

1.4 Vocabulary

Authorization: Prior, express, and informed consent from the Data Subject for personal data processing. Consent can be given in writing, verbally, or via unequivocal behaviors by the Data Subject that allow concluding that information was granted.

Privacy Notice: Verbal or written communication aiming to comply with the duty of informing an Interested Person regarding the activities, processing types, purposes, and other aspects associated with personal information management.

Database: Organized set of personal data subject to Processing and stored on manual or automated media, which contains clearly identified or identifiable information on individuals (e.g., worker database, vendor database, training attendance database, among others).

Successor: Person who has succeeded to another due to the latter's death (heir or legatee).

Personal data: Any information linked to or that could be associated with one or several identified or identifiable physical or individual persons.

Private Personal Data: Personal data the knowledge of which is restricted to the public.

Semi-private data: Data that is not of an intimate, reserved or public nature and whose knowledge or disclosure may be of interest not only to its owner but also to a certain sector or group of persons.

Public Data: Data that is not semi-private, private, or sensitive, that can be processed by any person, with no need for authorization to do so. Public data includes, among others, the data contained on a person's documents of vital statistics (e.g., married or single, male or female), and those contained on public documents (e.g., Public Deeds), public records, among others.

Sensitive Data: Data affecting the intimacy of the Interested party or the improper use of which could lead to discrimination, such as those revealing their racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social or human rights organizations, or organizations promoting the interest of any political party or guaranteeing the rights and guarantees of opposition political parties, as well as data related to health, and sex life. This data also includes biometric data, including fixed or moving images, digital fingerprints, photographs, iris, voice, facial, or palm-print recognition, etc.

Data Protection Delegate: Corporate role responsible for overseeing, controlling and promoting the application of the Corporate Personal Data Protection Program, as well as its continuous and sustainable improvement under the supervision of the European Union General Data Protection Regulation (GDPR) and other applicable provisions.

Area Privacy Appointees: Role assigned to an employee in each of the Company's different areas, that supports and coordinates with the Privacy Delegate for performing different internal activities and procedures for compliance with corporate and regulatory personal data protection provisions.

Profile Creation: Creation of individual decisions based on automated data processing aiming to evaluate a person’s personal aspects or analyze or predict their professional performance, financial situation, health, personal preferences or interests, reliability, behavior, location, or movements.

Data Processor: Public or private, individual, or corporate person who, either on their own or together with others, carries out Personal Data Processing on behalf of the Data Controller. For the purposes of this document, is understood as the partner or vendor that performs personal data processing under the auspices of a contract or agreement and according to the instructions, guidelines, and purposes defined by the Company.

Public Interest: Justification driving personal data processing as a function of one or several of the following events:

- Processing done by public Authorities or Entities in the course of their functions.
- Processing performed in the public interest and subject current legislation.
- Processing for the purposes of historical, statistical, or scientific research.

Data Controller: Public or private individual or corporate person that, individually or in association with others, makes decisions regarding the database and/or data Processing.

Data Subject or Interested Party: Physical individual whose personal data is subject to Processing.

Data Processing: Any operation or set of operations on personal data, including its collection, storage, use, circulation, or suppression, or any or all of these.

International Data Transfer: Transfer of data to persons, corporations, or other entities in third-party countries or international organizations not established in the Union’s territory. According to the Organization’s NCPDP guidelines, these transfers may be destined for a Data Controller (international data transfer) or a Data Processor (International transmission of personal data).

1.5 Related Documents

POLICIES
SIG_POL_002 Information Asset Acceptable Use Policy
SIG_POL_003 Information Classification Policy
SIG_POL_005 Remote Access Policy
SIG_POL_011 Mobile Device Security Policy
PROCESSES
N.A.
PROCEDURES

N.A.
INSTRUCTION MANUALS
N.A.
FORMS
N.A.

2. GENERAL PRINCIPLES, POSTULATES and SPECIFIC PRINCIPLES

GENERAL PRINCIPLES AND POSTULATES.

- TODO1 promotes the protection of rights including those related Habeas Data, privacy, intimacy, goodwill, honor, and personal image, such that all actions will be governed by the tenets of good faith, legality, information self-determination, freedom, and transparency.
- TODO1 acknowledges that its legitimate right to Process the personal data of Data Subjects must be exercised within a specific framework of the law, consent from the data subject, and the specific instructions given by Data Controllers when applicable, seeking at all times to maintain a balance between the rights and obligations of Data Subjects, Controllers, and other Data Processors connected to its operations.
- Whomsoever, in the course of their activities, should provide the Company, as Data Controller or Data Processor, with any kind of personal data or information, may exercise their rights as Data Subject to have knowledge of, update, and rectify their data, and to exercise any and all other rights granted by the GDPR according to the procedures defined in applicable regulations and this policy.

SPECIFIC PRINCIPLES

Todo1 will apply the following specific principles, which constitute the rules to be followed for the collection, management, use, Processing, storage, exchange, and suppression of personal data:

- Legality: Loyalty and transparency towards the Data Subject.
- Limitation of purpose: Collected for defined, explicit, and legitimate purpose, and not subsequently processed in a manner incompatible with that purpose.
- Data minimization: Adequate, pertinent, and limited as necessary for the purpose for processing.
- Precision: Updated without delay as regards the purpose for processing.
- Limited retention: Retained such that Data Subjects can be identified for the time necessary for the purpose for processing, and no longer, except if Processing is performed exclusively for archive purposes in the public interest or for historical, statistical, or scientific purposes.

- Integrity and confidentiality: Implementing appropriate technical and organizational measures to protect the data against unauthorized or illegal Processing, or accidental lost, destruction, or harm.
- Proactive responsibility: Being responsible and capable of proving compliance with all Processing principles.
- Systematic incorporation: Personal data protection principles will be implemented and extend to the interpretation of all TODO1's processes and procedures.

3. TODO1 PERSONAL DATA CONTROLLER AND DATA PROCESSOR

The following are the scenarios in which the Company has the condition of Data Controller or Data Processor as regards the different types of Data Subjects and as a function of its capacity to decide on the means or ends of Personal Data Treatment.

PROCESSOR:

TODO1 will act as Personal Data Treatment Processor whenever, in the course of its activities it uses or Processes personal information at the request of a third party acting as Data Controller for the processed data. According to the nature of the operation and the Company's corporate purpose, activities as Personal Data Processor will be performed mostly regarding the data of TODO1's client's user data, which is entrusted for providing contracted technological services and capabilities subject to the commercial service offerings that make up the Company's mission.

Although TODO1 has technical and operational autonomy for making decisions regarding the personal information, it may not decide regarding or dispose of the database as such or its Processing. For example: Suppress, share, or disseminate the database without prior consent or authorization from the Data Controller or the Data Subject. Thus, whomsoever should hold the title of Data Controller must accredit the legal basis or legitimate interest supporting the performance of Personal Data Processing activities required for fully performing the activities entrusted to the Company.

CONTROLLER:

TODO1 will act as Personal Data Controller whenever, in the course of its activities, it uses or Processes personal information and is directly responsible for informing the Data subject, and managing consent, the legal basis, or any other legitimate applicable event subject to applicable regulatory provisions.

4. PERSONAL DATA PROCESSING ACTIVITY LOG

In the course of its mission-related, strategic support, and related activities, the Company will perform Personal Data Management activities for the following categories of Data Subjects and Processing Activities, regarding which the Company acts as both Data Controller and Data Processor:

PROCESSING ACTIVITY LOG AS DATA CONTROLLER	
Subjects	Description of Processed Data
CLIENTS	<p>CLIENT CATEGORIES:</p> <ol style="list-style-type: none"> 1 Clients: Persons with which a commercial relationship for the provision of corporate services is maintained and which requires knowledge of data related to legal representatives and contact persons.
	<p>DATA TYPES</p> <ol style="list-style-type: none"> 1 General data related to their majority, date and place of birth, age, sex, nationality. 2 Identification data including names, surnames, DNI/NIF/Identification document, signature. 3 Commercial contact information: Address, telephone numbers, email. 4 Socio-economic data: Financial data, including tax data and economic activity, invoicing data.
	<p>PROCESSING PURPOSE:</p> <ol style="list-style-type: none"> 1 Commercial and administrative customer relations management.
	<p>LEGITIMATION:</p> <ol style="list-style-type: none"> 1 Contract execution 2 Consent
	<p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p> <ol style="list-style-type: none"> 1. Tax administration 2. Banks and financial entities 3. Hosting service providers or other technological services that support technical personal data processing and storage capacity.

	<p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES:</p> <ol style="list-style-type: none"> As provided in tax legislation for the limitation of liability.
	<p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST:</p> <p>International data transfer to corporations under the TODO1 Organization to provide technological and administrative support for the services provided by the Company.</p>
	<p>SECURITY MEASURES. See item 12.4</p>
SHAREHOLDERS	<p>DATA SUBJECT CATEGORIES:</p> <ol style="list-style-type: none"> Shareholders: Corresponds to persons with a share in the Company's stock no matter their shareholding percentage. <p>DATA TYPES</p> <ol style="list-style-type: none"> General data related to their majority, date and place of birth, age, sex, nationality. Identification data including names, surnames, DNI/NIF/Identification document, signature. Private and commercial contact information: Address, telephone numbers, email. Socio-economic data: Financial data, including tax data and economic activity, direct deposit information <p>TREATMENT PURPOSE</p> <ol style="list-style-type: none"> Management of commercial and corporate relations, and corporate and statutory affairs. <p>LEGITIMATION</p> <ol style="list-style-type: none"> Overriding legitimate interest of the controller. <ul style="list-style-type: none"> Relationship to the controller's activities. Legal obligation for the controller. <p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p>

	<p>1. Tax administration 2. Banks and financial entities 3. Hosting service providers or other technological services that support technical personal data processing and storage capacity.</p> <p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES: 1 As provided in tax legislation for the limitation of liability.</p> <p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST: International data transfer to corporations under the TODO1 Organization to provide technological and administrative support for the services provided by the Company.</p> <p>SECURITY MEASURES. See item 12.4</p>
<p>VENDORS</p>	<p>DATA SUBJECT CATEGORIES Vendors: Persons with which a commercial contract relationship exists for the acquisition of goods or services required by the Company in the course of its corporate purpose.</p> <p>DATA TYPES</p> <p>1 General data related to their majority, date and place of birth, age, sex, nationality. 2 Identification data including names, surnames, DNI/NIF/Identification document, signature. 3 Commercial contact information: Address, telephone numbers, email. 4 Socio-economic data: Financial data, including tax data and economic activity, direct deposit information</p> <p>PURPOSE OF PROCESSING 1 Manage commercial relationships with vendors</p>

	<p>LEGITIMATION</p> <ol style="list-style-type: none"> 1 Contract execution 2 Consent <p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p> <ol style="list-style-type: none"> 1. Tax administration 2. Banks and financial entities 3. Hosting service providers or other technological services that support technical personal data processing and storage capacity. <p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES:</p> <ol style="list-style-type: none"> 1 As provided in tax legislation for the limitation of liability. <p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST: International data transfer to corporations within the TODO1 Organization to provide technological and administrative support for the Company's corporate and statutory functions.</p> <p>SECURITY MEASURES See item 12.4</p>
<p>EMPLOYEES</p>	<p>DATA SUBJECT CATEGORIES:</p> <ol style="list-style-type: none"> 1 Employees: Persons with a direct relationship to the Company under an employment contract

	<p>2 Workers on assignment: Persons providing temporary services to the Company through a third party (employment agency)</p> <p>DATA TYPES</p> <ol style="list-style-type: none"> 1 General data regarding their majority, date and place of birth, age, sex, nationality. 2 Identification and contact data, including information related to their voice, photograph, video, signature. 3 Private and corporate contact data: Address, telephone, email. 4 Socio-economic data: Financial data, tax information, equity information, work-related data, level of education, work experience. 5 Bank data for payroll deposits 6 Police or disciplinary background information. 7 Password and IT system user information. 8 Sensitive Data associated with their occupational medical aptitude, disabilities, and relevant health information for complying with workplace risk and health prevention provisions.
	<p>PROCESSING PURPOSE</p> <ol style="list-style-type: none"> 1 Management of the working relationship with employees.
	<p>LEGITIMATION</p> <ol style="list-style-type: none"> 1 Contract execution
	<p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p> <ol style="list-style-type: none"> 1. Labor and tax authorities. 2. Healthcare providers. 3. Insurance companies. 4. Workplace risk and healthcare prevention providers. 5. Personal Data Processors and Human Resources 6. Hosting service providers or other technological services that support technical personal data processing and storage capacity.

	<p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES: As provided in tax and labor legislation for the limitation of liability.</p>
	<p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST: International data transfer to corporations within the TODO1 Organization to provide technological and administrative support for the Company's corporate functions.</p>
	<p>SECURITY MEASURES See item 12.4</p>
<p>VISITORS TO COMPANY FACILITIES</p>	<p>DATA SUBJECT CATEGORIES: 1 Visitors: Physical persons accessing physical Company locations for the performance of commercial or operational activities.</p> <p>DATA TYPES: 1 General data related to their majority. 2 Identification data including images, photographs, and video. 3 Private or commercial contact data: Telephone number</p> <p>PROCESSING PURPOSE 1 Physical security management and facility access controls</p> <p>LEGITIMATION 1 Consent 2 Prevailing legitimate interest of the Controller associated with physical facility security management and Company information</p> <p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED: 1. Legal authorities 2. Security entities and forces 3. Security companies</p>

	<ol style="list-style-type: none"> 4. Insurance companies 5. Workplace risk and healthcare prevention providers. 6. Hosting service providers or other technological services that support technical personal data processing and storage capacity. <p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES:</p> <ol style="list-style-type: none"> 1. 30 days after initial information collection <p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST:</p> <ol style="list-style-type: none"> 1. This information is not transferred internationally <p>SECURITY MEASURES: See item 12.4</p>
<p>COMMERCIAL AND WORK-RELATED CONTACTS</p>	<p>DATA SUBJECT CATEGORIES:</p> <ol style="list-style-type: none"> 1. Commercial contacts <ul style="list-style-type: none"> - Persons related to the company's activities 2. Work-related contacts <ul style="list-style-type: none"> - Persons under an employment contract with the Company or that provide temporary services to the Company 3. Institutional contacts: <ul style="list-style-type: none"> - Contact persons for entities and authorities related to the Company's activities <p>DATA TYPES</p> <ul style="list-style-type: none"> - Identification data: Names and surnames, electronic signature - Private and commercial contact data: Address, telephone numbers, email - Professional data: Position, functions

	<p>PROCESSING PURPOSE</p> <p>1 Communication with third parties regarding the company's activities.</p> <hr/> <p>LEGITIMATION</p> <p>1 Contract execution.</p> <ul style="list-style-type: none"> • Employment relationship. • Commercial relationship. <p>2 Prevailing legitimate interest of the controller.</p> <ul style="list-style-type: none"> • Relation to the controller's activities. <p>3 Legal obligation of the controller.</p> <ul style="list-style-type: none"> • Officials and public positions related to the controller's legal obligations. <hr/> <p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p> <p>1. Hosting service providers or other technological services that support technical personal data processing and storage capacity.</p> <hr/> <p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES:</p> <p>1 Foreseen until the end of their relationship with the company's activities</p> <hr/> <p>INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST:</p> <p>International data transfer to corporations within the TODO1 Organization to provide technological and administrative support for the Company's corporate functions.</p> <hr/> <p>SECURITY MEASURES: See item 12.4</p>
PROCESSING ACTIVITY LOGS AS PROCESSOR	
Data Subjects	Description of Processed Data

Client Users	<p>CLIENT CATEGORIES:</p> <ol style="list-style-type: none"> Client Users: Persons with whom the Company's clients have commercial relationships as clients or users of their financial services. <p>DATA TYPES</p> <ol style="list-style-type: none"> General data related to their majority, place and date of birth, age, sex, nationality. Identification data including names, surnames, DNI/NIF/Identification Document, signature, address, telephone numbers, email. Private and commercial contact data: Address, telephone numbers, email Socio-economic data: Financial data, tax data and economic activity, transactional financial data Other data: Data associated with purchases or consumptions performed by users via the Company's clients' platforms and transaction media, user information and passwords for accessing the Company's clients' transactional IT systems.
	<p>PROCESSING PURPOSE</p> <ol style="list-style-type: none"> Manage fulfillment of contractual obligations entrusted by the client Data Controller and associated with technical support and transactional information processing for its clients and users.
	<p>LEGITIMATION</p> <ol style="list-style-type: none"> Contract execution. Prevailing legitimate interest of the controller. <ul style="list-style-type: none"> Relation to the controller's activities.
	<p>CATEGORIES OF RECIPIENTS TO WHOM DATA HAS BEEN OR WILL BE COMMUNICATED:</p> <ol style="list-style-type: none"> Hosting service providers or other technological services that support technical personal data processing and storage capacity.
	<p>PLANNED DEADLINES FOR THE SUPPRESSION OF DIFFERENT DATA CATEGORIES:</p> <ol style="list-style-type: none"> Foreseen until the end of the contract relationship with the Client.

	2 Foreseen until the end of the commercial relationship between the Client and users as instructed by the Data Controller
	INTERNATIONAL DATA TRANSFER AND DOCUMENTATION OF GUARANTEES FOR EXEMPT INTERNATIONAL DATA TRANSFERS ON THE BASIS OF AN OVERRIDING LEGITIMATE INTEREST: International data transfer to corporations within the TODO1 Organization to provide technological and administrative support for the Company's corporate functions.
	SECURITY MEASURES: See item 12.4

5. MAIN SCENARIOS AND SPECIFIC PURPOSES FOR PERSONAL DATA PROCESSING

Personal Data Processing activities performed by the Company are associated with the specific scenarios and purposes described below:

1. Procurement Management:

- a) Verify commercial background, reputation, and potential relationship risks associated with Money Laundering and Terrorist Financing.
- b) Legally and commercially affiliate the vendor or partner to the Company, enabling the operation's accounting, logistic and financial procedures.
- c) Formalize the contract relationship with the vendor or commercial partner, controlling full performance of the obligations assumed.
- d) Evaluate the performance and results of the vendor or partner to strengthen contracting or procurement procedures.

2. Human Talent and Labor Relations Management:

- a) Verify commercial background, reputation, and potential relationship risks associated with Money Laundering and Terrorist Financing.
- b) Evaluate the employment profile of candidates for purposes of selection and formalization of the employment relationship, filling vacancies or personnel requirements in the Company's different areas and functions.
- c) Verify educational, employment, personal, family backgrounds and other significant socio-economic elements related to candidates for employment, according to the requirements of the position to be filled.
- d) Manage the affiliation or report events related to the social security system with the authorities, as well as any other work-related assistance and benefit obligations.

- e) Register workers with the Company's management IT systems, enabling the accounting, administrative, and financial activities inherent to the employment relationship.
- f) Manage work-related events that impact payroll settlement and payments.
- g) Promote wellbeing and comprehensive development activities for the worker and their workplace and family environment.
- h) Manage training and education programs according to corporate guidelines the requirements of each position.
- i) Manage the workplace security, prevention, and healthcare management system, fostering risk mitigation and adequate incident response.
- j) Evaluate worker performance and analyze functional competencies to define career paths and comprehensive development.
- k) Manage employment termination processes and comply with corresponding financial obligations.
- l) Manage the performance and fulfillment of operational and functional tasks associated with the position's profile.
- m) Apply internal procedures required to apply the provisions of the internal workplace regulations.
- n) Monitor compliance with labor obligations and appropriate use of the corporate tools provided by the Company, including communications, messages, and tracing files uploaded to and downloaded from corporate information systems and applications.
- o) Send semi-private information including payroll slips and competency evaluation results using the worker's private contact details to promote privacy of their personal information.
- p) Backup information managed on corporate systems and applications to guarantee registration of and access to historically relevant information on the Company's operations and the continuity of those operations even after employee termination.

- q) Use the employee's image and voice in different audiovisual media for broadcast over physical or digital corporate media.

3. Management of Commercial Relations with Clients:

- a) Verify commercial background, reputation, and potential relationship risks associated with Money Laundering and Terrorist Financing.
- b) Support commercial relations with clients and leads, enabling inclusion in the Company's management systems for the performance of the operation's accounting, logistic, commercial, and financial procedures.
- c) Manage client communication and loyalty activities, and attend to Requests, Complaints, Claims and Suggestions (RCCS) in a timely manner to evaluate the quality of the products and services offered by the Company.
- d) Carry out marketing and market intelligence activities to strengthen the Company's sales management.
- e) Invite, sponsor, or organize the participation of current or potential clients in commercial events or activities or events or activities promoting the services of the Company or its partners, potentially maintaining a record of attending Data Subjects on video, photographs, or any other physical or automated media.
- f) Deploy activities related to business intelligence, prospective clients, analytics, and market research and trends to improve the Company's knowledge of current or potential clients.
- g) Create and send behavioral advertising to its clients, i.e., advertising based on interests shared by clients on social media and/or during interactions with TODO1 and/or its partners.

4. Administrative, Governance, Risk and Compliance Management:

- a) Log and control access to Company facilities, mitigating physical security and information risks.
- b) Verify, control and monitor process, activity, and service performance according to guidelines and objectives defined by internal or external auditing.

- c) Verify, control and monitor process, activity, and service performance according to environmental, quality management, and information security management guidelines.
- d) Manage compliance with legal obligations and requirements associated with the course of the Company's operations.
- e) Manage claims of bad corporate practice or practices affecting corporate ethics or transparency.
- f) Support the operation's performance with concession, management, and maintenance of the Company's IT tools and applications.
- g) Manage the performance of jurisdictional or extra procedural actions or acts associated with alternative conflict resolution mechanisms, either on its own behalf or as a registered agent.
- h) Manage compliance with corporate and company obligations as regards internal bodies and external authorities.

5. Accounting and Treasury Management

- a) Enable controlling the Company's economic movements by recording accounting and causation receipts.
- b) Facilitate decision making and knowledge of the Company's economic situation for directors and other competent positions by generating reports, information, and indicators supported by aggregate or individual information.
- c) Comply with legal provisions that oblige the Company to submit financial reports and statements to the competent authorities.
- d) Define and implement control mechanisms associated with vendor payment validations
- e) Manage good relations between the Company and government entities with which it is obliged to stay in constant communication

6. DATA SUBJECT AUTHORIZATION AND CONSENT

Whenever personal information is collected by TODO1 in its capacity of Data Controller, the following aspects will be considered:

Means and Manifestations to Grant Authorization.

Required authorization for Personal Data Processing is obtained through requests and privacy notices made available to the Data Subject via each channel or point for capturing physical, verbal, or digital information, and provided through forms, notices, or declarations informing the Data Subject regarding the collection and subsequent Processing their personal data, and related purposes, rights, channels for enforcing their rights, and, if applicable, a way to access this policy.

The Data Subject's authorization from Data Processing must be given expressly and in the different manners provided for by the GDPR considering the nature of each different information collection channel, whether in writing, verbally, or through unequivocal actions or behaviors by the Data Subject.

Proof of Authorization

Data Processing authorizations collected in the course of the activities described in this policy will depend on the nature of the channel or information collection point. Effective proof of authorization for Data Processing will depend on the type of mechanism used to obtain authorization, for example, a signed form, a record of acceptance or of website access, a recording of a conversation, among others. In the event of acceptance through unequivocal behaviors, sufficient proof of acceptance by the Data Subject will be configured by the following elements:

- a) Model request for authorization made available to the Data Subject at the time of data collection.
- b) An express indication on the model authorization request of the unequivocal behavior by the Data Subject constituting authorization for Data Processing.
- c) Evidence of unequivocal behavior by the Data Subject, when it is feasible to accredit information supplied by the Data Subject or any other type of proof of express acceptance according to the nature of the channel.

Whenever sensitive personal information is collected, the Company will manage personal data processing authorizations, safeguarding evidence of written and explicit acceptance.

OBLIGATIONS OF THIRD-PARTY VENDORS

Without prejudice to the specific provisions agreed in each particular case, third-party Data Processors obligated towards Todo1 either contractually or conventionally are subject to compliance with the following personal data protection related obligations:

- a) Adopt, abide by, and update a Processing Policy or corporate personal information directives applicable to their operations.
- b) Adopt, abide by, and keep current an internal personal data processing policy and procedure manual, including policy enforcement elements.
- c) Define and maintain open channels for attending to potential personal data protection related questions and claims from Data Subjects in a full and timely manner. At least one physical address, one landline or mobile line, and one email must be provided for these purposes.

EMPLOYEE OBLIGATIONS

Without prejudice to obligations agreed in each particular case, direct and indirect workers or employees must comply with the following obligations:

- a) Have knowledge of and abide by this personal data protection policy and any other conditions, limitations, purposes, and rights they may have as Data Subjects, including the right to lodge requests, complaints, or claims related to the Processing of their personal data by the Organization. These rights may be exercised using the methods, mechanisms, and procedures described in item 11 of this policy.

- b) Safeguard the security of personal data subject to Processing. This activity will be performed on behalf of Todo1 and according to the principles that protect it.

7. DATA SUBJECT RIGHTS MANAGEMENT AND ATTENTION PROCEDURES

Data Subjects, their representatives, or their successors may exercise their rights related to the access, rectification, suppression, and portability of their personal data, their right to restrict and oppose Processing, and their right to not be subject to individual automated decisions via the following process:

- a) At any time, the Data Subject or their representative may freely make requests regarding the personal data subject to Processing by the Company, after accrediting their identity.
- b) Whenever the request is lodged by someone other than the Data Subject, their legitimacy or representation for acting on behalf of the Data Subject must be accredited.
- c) Requests received directly by any third party acting as a Data Processor for TODO1 must be submitted by these third parties to the Company by the next business day at the latest after receiving them at the email address provided for under item 11.1 of this policy. TODO1 will act in the same manner towards the corresponding Data Controller when acting as Data Processor.
- d) Requests must contain at least the following information:
 - The Data Subject's name and contact address or any other information for receiving the response.
 - Documents accrediting the identity and capacity of the representative as indicated for the following cases:
 - ✓ Data subject: Identification document.
 - ✓ Successor: Civil registration and identification document.
 - ✓ Legal representative in the case of minors:
 - Parents: Birth record and identification document.
 - Guardians: Legal sentence granting legal representation.
 - ✓ Legal Representative authorized by the Data Subject: Ample and sufficient power of attorney for lodging the request associated with the exercise of the right to be exercised.

- A clear and precise description of the personal data regarding which the petitioner is exercising their rights
 - A clear and precise description of the rights the petitioner, their successors or representatives wish to exercise.
 - Contribute any documentation supporting the petition if applicable due to the nature of the data.
 - Other elements or documents to help locate the personal data, as applicable.
- e) If the Data Subject should submit an incomplete request, TODO1 will request the Data Subject to remedy such deficiencies within five (5) business days of receiving the request.
- f) In the case of fully filled out requests, TODO1 will respond to petitioners within 30 calendar days of receiving the request. If the request cannot be attended within that period, the Data Subject will be notified within this period, stating the reasons for delay and indicating the date on which the request will be answered, which in may in no event be greater than 60 days over and above the additional periods, whenever the number of requests or the nature of the request requires disproportionate effort, and a notice and justification must be sent to the competent authority.

If required, the Data Subject may contact the TODO1 data protection channels to request a form for submitting a request, which will be considered as assistance or support provided to the Data Subject but not an obligatory requirement for exercising their rights.

If the decision is made to not proceed with the Data Subject's request, the reasons for inaction and the possibility of lodging a claim with a supervisory authority and seeking a judicial remedy must be informed without delay and within 30 days of receiving the request at the latest. (GDPR article 12.4).

Any and all information supplied by the Company (GDPR articles 13 to 22 and 34) within the framework of an exercise of the Data Subjects' rights must be provided freely. However, when

requests are excessively unfounded or excessive, especially due to their repetitive nature, the Company may:

- a) Charge a reasonable fee as a function of the administrative costs required to provide the information or the communication or to perform the actions requested, or
- b) Refuse to act regarding the request.

Management of request associated with the exercise of Data Subjects' rights will be governed by the following specific guidelines according to the type of right exercised by the Data Subject:

- a) For access rights (Art. 15), Data Subjects will be provided with the list of personal data disposed or, together with the purpose they have been collected for, the identity of the data recipients, retention periods, and the identity of the Data Controller with which they can request rectification, suppression, and opposition to Data Processing.
 - Scope. The petition containing the access request must specify whether the information requested is related to concrete data, data included in a given file or Process, or the entirety of the data subject to Processing.
 - Justification: Not required unless this right has been exercised within the last six months.
 - Refusal: Must be motivated and indicate that AEPD tutelage can be invoked. Motives for refusal may include: The right has already been exercised within twelve months prior to the request (unless a legitimate interest is accredited in this regard) and that this is provided under a Law or a regulation of directly applicable community law, or when these prevent the Data Controller from revealing the Processing of their data to the affected parties.
 - Approval: Notification to the Data Subject using the contact methods indicated in the petition.
- b) For rectification rights (Art. 16) imprecise or incomplete Data Subject data will be modified according to the Processing purpose.
 - Justification: Must indicate the data referred and the correction to be made. Supporting documentation must be submitted depending on the nature of the petition.
 - Refusal: Must be motivated and indicate that an appeal can be lodged with the AEPD.

- Approval: Notification to the Data Subject using the contact methods indicated in the petition.
- c) As regards the right to restriction of processing (Art. 18), Data Subject data will not be processed whenever:
- The accuracy of the personal data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the personal data;
 - The Processing is unlawful, and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - The Controller no longer needs the personal data for the purposes of the Processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
 - The Data Subject has objected to Processing pursuant to Article 21 (1) of the GDPR, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Personal Data Processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. 4.5.2016 L 119/44 Official Journal of the European Union ES.

A Data Subject who has obtained restriction of Processing shall be informed by the Controller before the restriction of Processing is lifted.

- Justification: Concurrence of well-founded and legitimate motives related to a concrete personal situation.
- Refusal: Must be motivated and indicated that an appeal can be lodged with the AEPD.
- Approval: Notification to the Data Subject using the contact methods indicated in the petition.

- d) As regards the right to object (Art.21): The data of Data Subjects will be blocked whenever they should indicate their refusal or opposition to give consent for Data processing and there is no legal obligation preventing this.
- Justification: Concurrence of well-founded and legitimate motives related to a concrete personal situation.
 - Refusal: Must be motivated and indicated that an appeal can be lodged with the AEPD.
 - Approval: Notification to the Data Subject using the contact methods indicated in the petition.
- e) For the right of erasure (Art.17): The Data Subject's data will be erased when they indicate their refusal or opposition to consent to their data being processed and there is no legal obligation preventing this and the Data Controller and Data Processor's responsibilities have expired.
- Justification: The data for cancellation must be indicated together with justification, providing documentation.
 - Refusal: Must be motivated and indicated that an appeal can be lodged with the AEPD.
 - Erasure will not proceed when personal data must be retained for periods provided for under applicable provisions, or, as the case may be, in the contract relationship between Data Controller and the Data Subject under which Data Processing is justified.
 - Approval: Notification to the Data Subject using the contact methods indicated in the petition.
- f) For the right to data portability (Art.20): Data Subjects must notify their decision and inform the Controller, as the case may be, regarding the identity of the new controller to whom their personal data must be provided. This data transfer will be feasible whenever:
- Processing is carried out by automated means.
 - Is technically possible.
 - Processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
 - The right will not negatively affect the rights and freedoms of others.

- g) For the right to not be subject to automated individual decision-making (Art.22): Data subjects must notify their decision and inform the Controller that they do not wish to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her
- The Controller must inform all persons with access to the personal data regarding the terms of compliance for attending to the Data Subjects' rights, and the manner and process for attending to said rights.

The Company will communicate any personal data rectification or suppression or restricted Processing according to article 16, article 17(1), and article 18 of the GDPR to each recipient to which personal data has been communicated, unless this is impossible or would require disproportionate effort. The Company will inform the Data Subject about these recipients, if requested to do so by the Data Subject.

CHANNELS ENABLED FOR DATA SUBJECTS TO EXERCISE THEIR RIGHTS

The Company has designated a third party as Personal Data Protection Delegate for managing and attending to Data Subject rights. This Delegate may be contacted over institutional channels shared from time to time with the organization and the public at large.

If Data Subjects should use other contact channels to exercise their personal data protection rights, the Company reserves the right to refer or inform the Data Subject regarding the existence of the previously described channels so consultation or claims procedures can be initiated in a timely and complete manner.

8. ON SPECIAL PROVISIONS FOR PERSONAL DATA PROCESSING AND ACCREDITATION OF "PROACTIVE ACCOUNTABILITY" PRINCIPLES

IDENTIFYING AND UPDATING THE PERSONAL INFORMATION CYCLE

For adequate compliance with the personal data protection regime, TODO1 will identify and keep current an understanding of the personal information lifecycle for its operations, specifically defining and validating the following elements:

- a) Activities or processes that initiate or justify Personal Data Processing.
- b) Personal information collection channels or points, describing the type of information collected, the means of collection, and the purpose for collection.
- c) Databases and other information repositories where the collected personal information is stored, specifying whether the data will be processed using physical or automated means.
- d) TODO1 users or internal areas with access to information in databases and other repositories of personal information, specifying the purposes of information use or access.
- e) Nodes or output points for personal information, identifying third-party recipients, type of third-party liability, and the national or international scope of information transmission or transfer.
- f) Disposal mechanisms for collected personal information.

THIRD-PARTY RELATIONS.

The Company will seek to become commercially affiliated or related to third parties that reflect their commitment to observing and applying applicable personal data protection obligations and requirements in their own operations.

Thus, without prejudice to the use of Processing authorization request forms or models, privacy notices, and precedent contract coverage, the Company may ask third parties for pertinent

information allowing it to verify compliance with the personal data protection provisions under this policy and those found in its own internal policies and procedures whenever necessary.

Prior to contract conclusion, third parties that, in the course of their contracted or conventional purpose, have an impact on Processing or on any part of the lifecycle of the Company's personal information must accredit compliance with the requirements of the data protection regime, including, without limitation, the existence and enforcement of a Personal Data Processing policy, the activation of channels for attending to Data Subject requests for exercising their rights, and effective creation and updating of personal data processing logs, among other obligations enshrined under the GDPR and other complementary provisions.

Likewise, the Company reserves the right to oversee third-party compliance with legal and contractual requirements associated with the personal data protection regime from time to time or periodically. For this purpose, it may request proof of or supporting documentation for compliance, visit third-party facilities or offices, among other measures considered reasonable according to the criticality of the operation, data volumes, or the nature of the contract's object.

Upon termination for any reason whatsoever of the legal, contractual, or commercial relationship between the Company and any third-party that has an impact on Personal Data Processing, pertinent procedures will be applied to guarantee safe and effective disposal of personal information subject to Processing. These will include suppression, restitution, dissociation, or any other activity considered pertinent by the Company.

In the event of full or partial breach of current personal data protection obligations or this policy by third parties under a contract or conventional relationship, the Company may, at its discretion, terminate for the contract or conventional relationship for cause, or, failing that, agree on an action plan aimed at achieving minimum legal compliance, so long as the contingency measures required to prevent serious risk to the rights of Data Subjects are adopted. If an action plan is agreed with the party for compliance with the personal data protection regime, this plan will be understood to be made a part of the contract or agreement that formalize the third-party relationship.

PRIVACY IMPACT REVIEW

The Company acknowledges the importance of privacy and of protecting the information of its Data Subjects within the framework of its operations. To promote sustainability and continuous improvement of current legal, technical, and organizational coverage, TODO1 has adopted an internal procedure to be applied prior to the development of new operations or initiatives that has an impact on its current Personal Data Processing cycle, to determine *ex ante*, or in advance, the actions, measures, and coverage required for information protection and appropriate Personal Data Processing.

Development of this proof-of-diligence initiative is coordinated by the Privacy Delegate, without prejudice to the cross-cutting responsibility acquired by all human resources affiliated with the Company regarding the procedures contained in TODO1's internal personal data processing policies and procedures manual.

Without prejudice to any specific requirements applicable to particular cases, privacy impact reviews must consider the impact and the legal, technical, and organizational implications and coverage of the following core elements:

- a) Impact on stakeholders
- b) Impact on third parties
- c) Impact on competent authorities
- d) Impact upon the Company
- e) Risk management

9. INFORMATION SECURITY AND PRIVACY RISK MANAGEMENT

Article 5.1.f of the General Data Protection Regulations (GDPR) establishes the need to define appropriate security guarantees against unauthorized or unlawful processing, and against accidental loss, destruction, or damage. This requires the implementation of technical and organizational measures to ensure the integrity and confidentiality of personal data and the capacity (article 5.2) to prove that these measures have been implemented (proactive accountability).

These active accountability measures are included within those the Controller must apply prior to starting and during Processing.

This type of measures directly reflects a proactive accountability approach. This approach requires thinking about data protection right from the moment a process, product or service implying personal data processing is designed.

OBLIGATIONS

- From the start, TODO1 must implement organizational and technical measures to guarantee that GDPR principles will be effectively applied within its processes.
- TODO1 must adopt measures to guarantee that only necessary data are processed (minimization) with regards to the amount of data processed, processing amounts, retention periods, and data accessibility.
- Technical and organizational measures must be established, considering:
 - Technical costs.
 - Application costs.
 - Processing nature, scope, context, and purpose.
 - Risks to rights and freedoms.

Minimum security measures can be found in the Company's internal personal data security and privacy directive (Item 10.6, internal personal data processing policies and procedures manual), which includes the following general guidelines:

Organizational Measures:

- Definition of staff functions related to their information management responsibilities:
 - ✓ Person responsible for security
 - ✓ System administrator
 - ✓ User
 - ✓ Personnel with no personal data processing responsibilities

- Obligations affecting all Company personnel:
 - ✓ Confidentiality obligations
 - ✓ Workstations
 - ✓ Safeguard and protect personal passwords
 - ✓ Incident management
 - ✓ Media management

- Administrative procedures:
 - ✓ Telephone requests for personal information
 - ✓ Paper disposal
 - ✓ Sending e-mails
 - ✓ Receiving CVs
 - ✓ Incident notification
 - ✓ Manual filing criteria
 - ✓ Payroll delivery
 - ✓ Temporary storage
 - ✓ Clean desk policy
 - ✓ Advertising mailings

Technical Measures: Include the measures and definitions associated with the following aspects:

- Processing centers and locations
 - ✓ IT system physical access measures

- ✓ Anti-theft system
- ✓ Fire suppression system
- ✓ Data protection center
- ✓ Electrical supply
- ✓ Climate control
- ✓ Paper file physical access measures
- ✓ Physical media destruction

- CCTV image capture
 - ✓ Camera location
 - ✓ Monitor location
 - ✓ Image retention
 - ✓ Duty to inform
 - ✓ Workplace control measures
 - ✓ Image access rights

- Workstation measures
- Operating and communications system environments
- IT system or applications to access processing
- Cloud service controls
- Personal password safeguards and protection
- Incident management
- Physical media management
- Backup and recovery management
- Data pseudonymization, anonymization and encryption

10. COMPREHENSIVE CORPORATE PERSONAL DATA PROTECTION PROGRAM

The Company has developed a comprehensive corporate personal data protection management and compliance sustainability program. This program has the following minimum components:

a) Organic component:

Includes the definition of roles and responsibilities for the Company's entire data protection management component, articulating different internal procedures with functional responsibilities and obligations and different operational administrative levels.

Without prejudice to the cross-cutting responsibility of each Company employee and director, the Privacy Delegate assumes the role of corporate personal data protection model coordinator.

The Privacy Delegate will report to the Legal Representative, Privacy Committee, or another instance representing upper management to enable strategic planning and information governance, specifically as regards the personal data protection and privacy policies.

b) Programmatic Component:

Includes an annual definition of the main programs, activities, and initiatives to be developed by the Company for the sustainability of the personal data protection management and compliance model under principles of accountability and continuous improvement.

The annual corporate personal data protection program will be submitted by the Privacy Delegate and approved by Legal Representative, Privacy Committee, or another instance defined by the Company in representation of upper management.

Without prejudice to the inclusion of other elements, the annual corporate personal data protection program will include and implement the following activities:

- Training for Company personnel.
- Operational support for analyzing legal, technical, and organizational coverage associated with Data Subjects, third parties, and the authorities.
- Internal verification, controls, and measurement.
- Formulation of improvement plans and actions, including following-up and supporting their implementation.
- Compliance with external reports to and monitoring of the regulatory environment.
- Submission of annual reports to Upper Management on the current status of the personal data protection management and compliance model.

11. CCTV SYSTEM

To protect its financial interests and promote security throughout its facilities has designed a protocol for requesting, accessing, reviewing, and potential delivery of personal information captured by internal and/or external CCTV cameras.

The Company will ensure the custody and availability of video surveillance images according to its technical capacities and to requests received to review images that comply with its protocol.

12. FINAL PROVISIONS

AMENDMENTS TO THE POLICY

THE COMPANY reserves the right to modify this policy at any time. For this purpose, it will publish a notice on its website five (5) days prior to implementation and throughout the time the policy is current. If Data Subjects do not agree with new personal data management policies, they or their representatives may exercise their rights as Data Subjects under the aforementioned terms.

Databases containing personal data will be effective during the time the data therein is used and maintained for the purposes described in this policy. Once this (these) purpose(s) is (are) completed and there is no legal or contractual duty to retain the information, their data will be suppressed from our databases.

13. APPLICABILITY

This policy is included in the TODO1 Information Security Management System and security policies and, as such, applies to all TODO1 Collaborators and to third parties (and their proxies) that interact with the businesses and use TODO1 networks, information, and/or technology.

Violations of this policy may give rise to disciplinary action up to and including termination of the employment contract.

In the event of any violation by a contractor and/or vendor, the corresponding contract or service may be considered terminated.

These guidelines are part of the TODO1 Security Policies and are published and available on the intranet. A copy is provided to all Employees and to any and all third parties interacting with TODO1 businesses, networks, information, and/or technology.

A Letter of Acknowledgement must therefore be accepted and signed by all Employees, contractors, and/or vendors as a condition of their relationship towards TODO1.

This policy applies to all personal data processing activities performed by TODO1 throughout the territories where it has a presence, and to all personal data processing activities performed or promoted by the organization that require transferring or deploying personal data flows towards third party Data Controllers or Processors headquartered outside those territories. This document must be applied by all Company employees, partners, and vendors.

This policy embraces the Organizations NCPDP directives without prejudice to their preferential and specific application to personal data processing activities performed or promoted by TODO1 under the corporate principles of cooperation and consistency that govern personal data processing amongst corporations related to the Organization.

Any person external to the Company with access to or processing personal data under their responsibility or assigned to them, must formally state their knowledge of the Organization's current personal data processing policy.

Review Timetable

The TODO1 Security Committee must review these policies at least once a year and after any significant change that could affect information security management, thus making sure that policies are continuously updated and aligned with business objectives.

If any review is required outside this timetable, it will follow all TODO1 internal policy approval and change procedures.

14. REGISTRATION CONTROL

Form used	Personal Data Protection Policy
Code	SIG_POL_004
Source Registration	SIG_POL_004 Personal Data Protection Policy
Classification Level	For Public Use
Registration Type	Digital
Person Responsible for Preparation	Security Operations Director
Storage	https://todo1jira.atlassian.net/wiki/spaces/TODO1/pages/1277657985/Sistema+de+Gesti+n+de+Seguridad+de+la+Informaci+n
Access	All TODO1 employees
Conservation Period	Ongoing
Person Responsible for Conservation	To be defined
Final Disposal	As established for documents classified as For Public Use.