MSLA-ID
Your IDV Partner in Latin America

Privacy and Data Protection Compliance Program

Content

Introduction..3

Definitions 3

Regulatory Framework 5

Scope of application..6

Guiding principles on the protection of personal data 7

Security measures 13

1. INTRODUCTION

The Personal Data Security Document defines the procedures that must be implemented at **MSLA ID** (or indistinctly and hereinafter, **MSLA),** in order to achieve an optimal level of compliance with the Personal Data Protection Law No. 297331, its Regulations approved through Supreme Decree No. 003-2013-JUS2; and other international regulations (GDPR & CCPA).

In order to guarantee the security conditions required in terms of personal data protection, it is vital that those obliged to comply become familiar with the current legal framework; commit to providing the resources and direction geared towards effective law enforcement; understand the institutional context in the processing and protection of personal data (organizational, technological, legal, contractual, regulatory, physical, etc.); and clearly determine appropriate organizational roles and responsibilities with sufficient authority and resources to lead and enforce the security policy for the protection of personal data.

This Personal Data Security Document details the security measures, the flow of data, and all the processing of personal data that MSLA ID uses to provide its services to third-party client companies local and international.

In order to determine the aforementioned security measures, the nature of the personal data involved, the resources available to the Data Controller, the provisions of the Personal Data Protection Law, its Regulations, and the recommendations issued by the National Personal Data Protection Authority through the Security Directive have been taken into account.

In accordance with its status as Data Controller, MSLA ID will adopt and implement security, organizational, legal, technical and specific measures, ensuring the security and integrity of the resources, databases and personal data that are processed in the company.

Finally, the Personal Data Security Document is a dynamic instrument, and reflect the real situation of the organization.

2. DEFINITIONS

For the purposes of this Personal Data Security Document, the following definitions are established reflected in Law No. 29733, its Regulations and other complementary regulations:

2.1. Authorized access: authorizations granted to a user for the use of the various resources.

2.2. Authentication: A procedure for verifying a user's identity.

2.3. Personal data bank: an organized set of personal data, automated or not, regardless of the medium, whether physical, magnetic, digital, optical or others that are created, regardless of the form or modality of their creation, formation, storage, organization and access.

2.4. Non-automated personal data bank: a set of data of natural persons that is not computerized and structured according to specific criteria, which allows access to personal data without disproportionate effort, whether centralized, decentralized, or functionally or geographically.

2.5. Blocking: The identification and storage of personal data once the purpose for which they were collected has been fulfilled, with the sole purpose of determining possible liabilities in relation to their processing, until the legal or contractual limitation period for these. During this period, personal data may not be processed and after this period, it will be deleted from the corresponding database.

2.6. Cancellation: the procedure by which the controller ceases to use the data. The cancellation will imply the blocking of the data, consisting of the identification and reservation of the same in order to prevent its processing except for its availability to the Public Administrations, Judges and Courts, for the attention of the possible liabilities arising from the processing and only during the limitation period of such responsibilities. Once this period has elapsed, the data must be deleted.

2.7. Transfer or communication of data: any disclosure of data made to a person other than the data subject.

2.8. MSLA: indistinctly, MSLA ID, or MSLA

2.9. Consent: Manifestation of the will of the owner of the data by means of which the processing of the data is carried out.

2.10. Password: Sensitive information, often consisting of a string of characters, that can be used in the authentication of a user.

2.11. Access control: a mechanism that, depending on the identification already authenticated, allows access to data or resources.

2.12. Backup copy: Copying data from an automated database to a medium that enables its recovery.

2.13. Personal data: numerical, alphabetical, graphic, photographic, acoustic, personal habits, or any other type of information concerning natural persons that identifies them or makes them identifiable through means that can reasonably be used.

2.14. Health-related personal data: information concerning an individual's past, present, or predicted physical or mental health, including the degree of disability and genetic information.

2.15. Sensitive data: information relating to personal data referring to physical, moral or emotional characteristics, facts or circumstances of your affective or family life, personal habits that correspond to the most intimate sphere, information relating to physical or mental health or other analogous information that affects your privacy.

2.16. Recipient or transferee: the natural or legal person, public or private, or administrative body, to whom the data is disclosed.

2.17. Days: Business days.

2.18. General Directorate of Personal Data Protection: This is the body in charge of exercising the National Authority for the Protection of Personal Data referred to in Article 32 of Law 29,733, and any of these names may be used interchangeably.

2.19. Dissociation: The procedure by which personal data cannot be associated with the owner or allow, due to its structure, content or degree of disaggregation, the identification of the owner.

2.20. Document: any writing, graphic, sound, image, or any other kind of information that can be treated in an information system as a distinct unit.

2.21. Data Processor: The natural or legal person who, alone or jointly with others, processes personal data on behalf of the Data Controller.

2.22. Incident: Any anomaly that affects or could affect data security.

2.23. Law: Law No. 29733 on the Protection of Personal Data.

2.24. Organizational security measures: A set of actions and mechanisms to establish the management, support and review of information security at the organizational level, the identification and classification of information, as well as the awareness, training and training of personnel, in terms of personal data protection;

2.25. Legal security measures: a set of actions and mechanisms to ensure compliance with the principles of personal data protection and the movement of data outside the entity.

2.26. Technical security measures: A set of actions and mechanisms, whether or not they employ technology, aimed at: a) Preventing unauthorized access, damage, or interference to physical facilities, critical areas of the organization, equipment, and information; (b) Protect mobile equipment, portable or easily removable, located inside or outside the premises; c) Provide equipment that contains or stores personal data with maintenance that ensures its availability, functionality and integrity; d) Ensure the secure deletion of data; (e) Ensure that access to logical databases or information in logical format is by identified and authorized users; (f) Ensure that logical access is profile-compliant; g) Ensure that actions are included for the acquisition, operation, development and maintenance of secure systems, and h) Carry out the management of communications and operations of the computer resources used in the processing of personal data.

2.27.User profile: Authorized access to a group of users.

2.28.Person: Any natural person whose identity can be determined, directly or indirectly, by any information. An identifiable person is not considered to be an identifiable person when disproportionate deadlines or activities are required to achieve the identity of that person.

2.29.Regulation: Regulation of Law No. 29733 on Data Protection.

2.30.Data Controller: This is the person who decides on the processing of personal data, even if it is not in a personal data bank.

2.31.Security Officer: person(s) to whom the Data Controller has formally assigned the coordination and control of security measures.

2.32.Information system: a set of automated databases, programs, media and equipment used for the storage and processing of personal data.

2.33.Medium: a physical object that can be processed in an information system and on which data can be recorded or retrieved. Likewise, paper, photographic material, etc., are also included by support.

2.34.Deletion: Activity consisting of eliminating, erasing or destroying the personal data(s), once the blocking period has ended, under the security measures previously established by the responsible party.

2.35.Third: The natural or legal person, national or foreign, other than the owner or the person responsible for the data.

2.36.Legitimate interest: when the processing takes place within a client relationship, when it processes personal data for direct marketing purposes, to prevent fraud or to ensure the network and information security of your IT systems.

2.37.Data Subject: The natural person to whom the personal data corresponds.

2.38.Processing: The collection, use, disclosure or storage of personal data, by any means. The use includes any action of accessing, handling, exploiting, transferring or disposing of personal data.

2.39.Transfer: Any communication of data made to a person other than the data controller or processor.

2.40.User: Authorized subject to access personal data, databases or resources.

3. REGULATORY FRAMEWORK

The following is the regulatory framework and reference documents that are applicable for the

adaptation of MSLA ID to the protection of personal data, as well as various corporate

internal compliance documents.

The corporate documents, in addition to reflecting MSLA ID's commitment to IT security, provide an adequate framework for the simple establishment of protection measures for the processing of personal data.

4. SCOPE OF APPLICATION

The scope of application of this Personal Data Security Document is defined according to three basic criteria:

- ∇ Taking into account the place where the measures that are established through it are going to be implemented, the Material Scope will be determined.
- ∇ Taking into account the persons who must comply with the provisions of this Document, the Personal Scope will be delimited.
- ∇ Taking into account the company's resources on which the planned security measures are going to be applied and effectively implemented, the Functional Scope will be established.

4.1. MATERIAL SCOPE

This Personal Data Security Document will be applicable to MSLA ID, in its capacity as a company incorporated in national territory and Responsible Owner of the Personal Data Bank, with legal address and main place of business at Paseo de la Castellana 18, Madrid.

The Personal Data Security Document extends its scope of application to MSLA's headquarters and administrative sites.

4.2. PERSONAL SCOPE

The following persons are obliged to comply with the legal requirements contained in the Personal Data Security Document:

- Those who provide services, either directly or indirectly, for MSLA ID, regardless of the nature of the legal relationship that unites them with it.
- Any person who, due to the work they perform, has or may have access to the facility where the information system through which personal data is processed is located.
- Any person who, due to the work they perform, has or may have logical access to the digital environment where personal data is hosted, regardless of the medium it contains.
- Any person who, due to the work they perform, has or may have physical access to files, files, formats, spreadsheets, forms and documents that contain personal data in paper and/or automated format, related to any of the activities carried out by MSLA ID

MSLA ID is responsible for the task of training and informing people who, due to their status as users, are under the scope of application of this Personal Data Security Document, about the adequate compliance with what is established herein. Likewise, the Security Manager and DPO will be instructed to carry out the functions entrusted to them.

MSLA ID has established a list of users with access to the personal data contained in the databases processed by it.

The provisions of this Document shall apply, to the extent that they are affected, to those service providers to whom the processing of personal data has been delegated, within the framework of powers granted in the regulations on the protection of personal data.

4.3. FUNCTIONAL SCOPE

The provisions of this Document shall apply to all resources, information systems and media (automated or not) through which personal data in MSLA ID's databases are processed.

These resources are as follows: servers; other operating systems, installed applications, and cloud applications, to access and/or host personal data; desktops, notebooks, and mobile devices; external network connection (VPN, WIFI); printers, scanners, camcorders; any magnetic media for copying or storing data (CDs, DVDs, pen drives, disks, memory sticks, tapes, etc.); and any hardware/manual for data storage (paper).

5. GUIDING PRINCIPLES ON THE PROTECTION OF PERSONAL DATA

5.1. PRINCIPLE OF LEGALITY

The capture and processing of personal data carried out by MSLA ID will be subsumed as a whole in the provisions established in Law 29733 on the Protection of Personal Data and other applicable regulations, offering the data holders a reasonable expectation of privacy and adjusting the treatment to the current regulatory framework.

The Data Controller shall also comply with the prohibition of collecting personal data by fraudulent, unfair or unlawful means.

In order to duly comply with the principle of legality, the Data Controller will identify the main flows that consume personal data within the company, in order to be able to determine which security measures are applicable and the procedures, policies and good practices that must be developed and implemented.

5.2. CONSENT PRINCIPLE

As a general rule, all processing is subject to the consent of the owner, except for the exceptions regarding our IDV services to clients worldwide. Proof of receipt of consent is the responsibility of MSLA INTERNATIONAL, and may be revoked at any time without retroactive effect.

The request for consent must refer to a specific processing or series of processing, with express identification of the purpose or purposes for which the data is collected; as well as the other conditions that concur in the treatment or treatments, and meeting all the requirements required by Law to consider the consent as valid.

When it is required to capture the consent of the data subject, the Data Controller will arbitrate the means for the affected party to provide free, prior, express, unequivocal, and informed consent.

MSLA ID is made up of several administrative areas. There are no areas that process their own exclusive personal data banks, but rather different areas process the same personal databases, but with different levels of access privilege and for different purposes.

Thus, at MSLA ID there are seven large personal databases: Workers; Suppliers, Customers, Website Users, Complaints and Claims, Applicants and Video Surveillance.

Regarding the group of people affected by a selection process, candidates send their CVs to the company through advertisements published on various job platforms. Express consent is considered to be that which is manifested through the conduct of the owner that shows that he has unequivocally consented, given that otherwise his conduct would necessarily have been different. In the case of the digital environment (website users and complaints and claims), the statement consisting of "clicking", "clicking" or "clicking", "tapping a touch", "touch" or "pad" or other similar is also considered express. Thus, both the conduct of the holder, through the voluntary action of sending a CV and participating in a selection process, as well as when answering the job offer advertisement published by MSLA ID on the various job platforms, is considered an express manifestation of consent.

In the event that any sensitive data is collected, the Data Controller must arbitrate the means to, in the first job interview, provide the candidate with the Privacy Notice, so that the affected party consents in writing and by reliable means to the processing of their sensitive personal data.

In relation to the group of "workers", who make up the Human Resources personal database of MSLA ID, although the contractual relationship that unites them to employee and employer derives a tacit consent, a format must be implemented to capture the consent of sensitive employee data, among which the use of their biometric fingerprint for time control in the attendance system has been identified.

In the case of sensitive data (fingerprint, health data, income), consent must be given in writing, through a handwritten signature, digital signature or any other authentication mechanism that guarantees the unequivocal will of the data subject.

In addition, they must notify the duration of the data processing.

5.3. PRINCIPLE OF PURPOSE

Personal data must be collected for a specific, explicit and lawful purpose. The processing of personal data must not be extended to any purpose other than that which has been unequivocally established as such at the time of collection, excluding cases of activities of historical, statistical or scientific value when a dissociation or anonymization procedure is used.

A purpose is considered to be determined when it has been clearly expressed, without room for confusion and when the purpose of the processing of personal data is objectively specified.

MSLA ID does not process personal data for purposes other than those for which the data was collected and is subject to specific purposes.

In the case of personal data banks that contain sensitive data, as is the case of employee time control, it is expressly stated that their creation responds to this strict purpose, which is legitimate, specific and in accordance with the explicit activities or purposes of time control of the employees of MSLA ID

It is noted that, if the data is processed for a purpose other than those established, the Data Controller must again request the consent of the owner of the data.

The owner may deny or revoke his/her consent or oppose the processing of his/her data for purposes other than those that are necessary and give rise to the legal relationship established with the data controller, without this implying the termination of the processing of the data for the main purposes indicated.

5.4. PRINCIPLE OF PROPORTIONALITY

The data collected are adequate, relevant and not excessive, in relation to the purposes for which they have been obtained.

5.5. QUALITY PRINCIPLE

The personal data to be processed must be truthful and accurate; necessary, relevant and appropriate, and, as far as possible, up-to-date. They must be kept in such a way as to ensure their safety and only for as long as necessary to fulfil the purpose of the processing. It is presumed that the data directly provided by the owner or third-party provider of the same is accurate.

The data is kept for five (5) years, in accordance with the legal term. They keep employee files in the offices of the Human Resources area for the duration of the employment relationship. Once completed, it is filed in the filing room located in MSLA's main office. After five (5) years, the records are permanently deleted.

In accordance with labor legislation, Article 21 of Supreme Decree No. 001-98-TR provides that "Employers are obliged to keep their payrolls, duplicate receipts and the corresponding certificates for up to five years after payment has been made. After the expiry of the aforementioned period, the proof of the rights that may derive from the content of the aforementioned documents will be the responsibility of the person who alleges the right."

In accordance with labor and social security legislation, Legislative Decree No. 1310 specifies in paragraph 3.4 that "(...) For all legal purposes, employers are obliged to keep documents and proof of payment of economic labor obligations only until five years after payment is made.

Regarding employees' health data and compliance with biosecurity protocols for COVID-19, the medical information of the staff is updated in accordance with current technical regulations. Likewise, health and biosafety information is kept in physical form and in the formats of the Ministry of Health following the legal deadlines, in accordance with the regulations that regulate the matter.

In accordance with Article 8 of the Personal Data Protection Act, in accordance with the principle of proportionality, MSLA ID establishes deadlines and measures for the retention of personal data.

With regard to the Personal Data Bank of Customers and Suppliers, in accordance with Article 8 of the Personal Data Protection Act, in harmony with the principle of proportionality, MSLA ID establishes deadlines for the retention of personal data.

In order to establish periods for the retention of personal data, it will take into consideration:

- That MSLA ID's databases except the IDV services correspond to the category of INTERMEDIATE and provide that the purpose of the data processing is fulfilled within an indeterminate period or greater than one (01) year.
- That MSLA ID's databases regarding the daily transactions of IDV services for local and international clients, the purpose of the data processing is fulfilled within an indeterminate period or greater than one (01) month.

- Regarding the statute of limitations, Article 43 provides that "The action of the Tax Administration to determine the tax obligation, as well as the action to demand its payment and apply penalties, prescribes after four (4) years, and after six (6) years for those who have not filed the respective return. Such actions are time-barred after ten (10) years when the withholding or collection agent has not paid the tax withheld or received (...)". The foregoing means that taxpayers are OBLIGED to: Store, file and preserve the books and records, kept manually, mechanized or electronically, as well as the documents that constitute facts that may generate tax obligations while the tax is not prescribed. Statutes of limitations are set at 4, 6, and 10 years.
- Regarding the Video Surveillance Personal Data Bank, they are stored in a digital video recorder (DVR) that records according to each location, maximum up to 30 calendar days.

In order to comply with the principle of quality, MSLA ID will periodically review the data processed, so that they are accurate, complete, pertinent and, above all, up-to-date, both in paper and digital formats.

In order for the physical deletion of documents to coincide with the purging of digital documents, MSLA ID must devise the means to foresee that the information in paper format in conditions to be deleted can also be cancelled, blocked and/or deleted from the servers and computer platforms with which such information is managed.

Likewise, and in order to avoid duplication of information, as well as its outdatedness, all digital media that are prepared to carry out tasks (Excel spreadsheets, etc.) that contain personal data, must be hosted on the server, and eliminated as the purpose for which these data have been collected is exhausted.

In order to comply with the principle of quality, MSLA ID, as well as its collaborators, will periodically review the data processed, so that they are accurate, complete, pertinent and, above all, up-to-date.

5.6. SAFETY PRINCIPLE

The owner of the personal data bank and the person in charge of its processing must adopt the technical, organizational and legal measures necessary to guarantee the security of the personal data. The security measures must be appropriate and commensurate with the processing to be carried out and the category of personal data concerned.

In order to duly comply with the principle of security, MSLA ID, by means of this Security Document, will define the legal, organizational and technical measures that must be implemented for its personal data banks of category "INTERMEDIATE", in accordance with Information Security Policy -MSLAID in the Processing of Personal Data of the Directive issued by the General Directorate of Personal Data Protection.

5.7. PRINCIPLE OF RECOURSE PROVISION

The owner of personal data may exercise the rights of information, access, rectification, cancellation, opposition and objective processing of personal data before the Data Controller. The exercise of one or more of the rights does not exclude the possibility of exercising one or more of the others, nor can it be understood as a prerequisite for the exercise of any of them.

All holders of personal data must have the necessary administrative or jurisdictional channels to claim and enforce their rights, when these are violated by the processing of their personal data.

Within section 9 of this Personal Data Security Document, MSLA ID establishes the way that will be enabled for the holders of personal data to exercise their fundamental rights to the protection of personal data.

It is a clear and simple procedure to respond to requests to exercise the rights of the owners, designating a person responsible for dealing with them, who is aware of the rights of those affected in terms of data protection, and who has the necessary tools to respond to them.

5.8. PRINCIPLE OF APPROPRIATE LEVEL

MSLA ID currently carries out cross-border flow of personal data. In the case of the cross-border flow of personal data, it guarantees a sufficient level of protection for the personal data to be processed or international standards on the matter.

6. SECURITY MEASURES

This section details and describes the security measures aimed at ensuring the correct implementation of a Personal Data Security Management System and, through it, compliance with the legislation on Personal Data Protection and Third Party Information Security Risk Management-by MSLA ID.

It is noted that in order to effectively maintain the security measures, the Responsible Party may carry out the security functions by itself, or hire a natural person for this purpose.

For the determination of technical, organizational, legal (or legal) and specific security measures, the risk inherent to the quality of the personal data compromised and its criticality have been taken into account; the technological resources available to MSLA ID, and the possible detrimental consequences of a breach for the holders.

6.1. LEGAL SECURITY MEASURES

a. CONFIDENTIALITY

Each agent with access to personal data shall sign a commitment to secrecy and confidentiality with respect to the personal data that he or she processes in the course of his or her duties.

Agents will be expressly prohibited, for the duration of the contractual relationship, as well as once it has been terminated, to communicate procedures, personal data, valuation reports and, in general, any personal data that they have learned either by reason of their work in or for the entity, or for any other reason. The obligation of secrecy shall continue beyond the termination of the relationship between the agents and the Data Controller.

Likewise, the Data Controller must arbitrate the means to implement the confidentiality and personal data protection clause.

Finally, third-party data access agreements must include a confidentiality clause as detailed on Third Party Information Security Risk Management-MSLAID.

b. DUTY TO INFORM

The owner of personal data has the right to be informed in detail, simply, expressly, unequivocally and prior to its collection, about the purpose for which his or her personal data will be processed; who are or may be the recipients, the existence of the database in which they will be stored, as well as the identity and address of the data subject and, if applicable, of the person in charge of processing their personal data; the mandatory or optional nature of your replies to the questionnaire proposed, in particular with regard to sensitive data; the transfer of personal data; the consequences of providing your personal data and your refusal to do so; the length of time for which your personal data is retained; and the possibility of exercising the rights granted to them by law and the means provided for doing so.

It is the obligation of the Data Controller to inform the owner of the data of the information regarding the existence and characteristics of the processing to which their data will be subjected.

In order to comply with the duty to inform, MSLA ID will have different Privacy Notices, which were prepared in accordance with the purposes of the processing of personal data, the quality of the data processed and the groups of affected interested parties.

Thus, the entity has a General Privacy Notice for all the holders of the personal data that are in the register of the databases registered by MSLA, with the exception of the privacy notice for the registration of the database of web users, and the privacy information sheet of the registration of the video surveillance database.

The Human Resources Notice includes information for those who are part of a selection process within the company, and that if successful, it will swell the entity's human resources databases. To implement the Privacy Notice for Personnel Selection, the Head of the Personal Data Bank will insert a link with the content of the Notice, using any of the following options:

- Within the notice published on the various work platforms;
- Within the email that is sent to the interested party to arrange the first interview;
- By giving you the physical format of the Privacy Notice when you go to the first interview with human resources.

Regarding the collection of employees' personal data, together with the signing of the employment contract, they will be given the form of Privacy Notice and Request for Consent for Sensitive Data. The form of the Privacy Notice will be signed by the employee. They will then be scanned and archived.

In relation to the Privacy Notice for Customers and Suppliers, it will be included as a signature footer for emails.

As for the users of the website, it will be indicated in the interface of the website in a column where the legal notice is indicated or the legal documents of the company are listed, in order to comply with the duty to inform.

Finally, the Data Controller will have a Privacy Notice upon entering the MSLA INTERNATIONAL headquarters, in order to comply with the duty to inform regarding the access control and video surveillance database.

c. REGISTRATION OF PERSONAL DATA BANKS

Natural or legal persons from the private sector or public entities that create, modify or cancel personal data banks are obliged to process the registration of these acts with the National Registry for the Protection of Personal Data.

MSLA ID is made up of different administrative areas. There are no areas that process their own exclusive personal data banks, but rather different areas process the same personal databases, but with different levels of access privilege and for different purposes.

Thus, we find that in MSLA ID there are seven large personal databases: Workers; Suppliers, Customers, Website Users, Applicants, Complaints and Claims and Video Surveillance.

The Personal Data Bank for Worker Management is processed by the area of:

- ∇ Human Resources, being the primary person responsible for the information, the one that captures the personal information of the employees and the one that holds the greatest privileges over the personal data of the employees for the management of human resources of the entity;
- ∇ Administration, which accesses employee payrolls in order to make salary payments, control of employees' schedules, as well as other payments related to the employee's activity such as hotels, mobility, refreshments, etc.
- ∇ Accounting, which carries out an accounting control prior to authorizing the payment of payrolls;

The Personal Data Bank of Customers and Suppliers, which includes the B2C and B2B datasets of MSLA ID's customers as well as third-party organizations.

The Personal Data Bank of Users of the website, which includes the management of the data of users who are consumers of **MSLA products** and potential customers of MSLA ID, to which the marketing and sales area access information in order to send information.

The Applicants' Personal Data Bank is processed by the human resources area, which may store the documents submitted by the people who send information through the company's calls, in order to process the data for that purpose.

The Personal Data Bank of Complaints and Claims is processed in the digital environment – the company's website and is managed by the data entered by consumer users for the registration of complaints and claims of the MSLA products.

The Video Surveillance Personal Data Bank, which includes the management of the control of entry and exit of the entity, control of physical access of visitors, control of temporary exits, which must be declared to the General Directorate for the Protection of Personal Data of employees, control of video surveillance systems (cameras) installed at the company's headquarters.

The six identified personal data banks have been duly registered in the Register of Personal Data Banks by the Directorate-General for Personal Data Protection.

d. DATA RETENTION PERIODS

Personal data must be kept in such a way as to ensure its security, and only for the time necessary to fulfil the purpose of the processing. Since MSLA ID's databases correspond to the category of INTERMEDIATE, it is expected that the purpose of the data processing will be fulfilled in an indeterminate period or greater than one (01) year.

Regarding the retention period of the records stored in the Human Resources Personal Data Bank, the maximum period of data retention and duration of the processing has been established as five (5) years, in accordance with the legal term. Health data is kept in accordance with legal deadlines, in the custody of the primary information controller (physician), within the topic.

Regarding the Identity Data Verification services, the retention periods for daily transactions through AWS has been set at thirty (30) days.

For the Personal Data Bank of Website Users and for complaints and claims, the retention periods established by Law are also respected. For the rest of the data that is not subject to a legal retention period, the maximum retention period has been set at five (5) years.

Establish deadlines for the retention of the personal data of customers and suppliers who manage the areas of Sales, Logistics, Accounting and Administration.

Regarding the Video Surveillance Personal Data Bank, and in order to unify criteria, the retention period is established at five (5) years.

e. DUTIES OF THE CONTROLLER

MSLA ID, in its capacity as Responsible for the Personal Data Bank, is the only one empowered to decide on the purpose, content, use and processing of personal data, whose owners are the natural persons affected by the processing.

The Data Controller is responsible for complying with the security measures that must be adopted with respect to the personal data processed; the custody of databases, their backups and the control of their archive and availability.

The following are the obligations legally attributed to MSLA ID, as a Data Controller:

1) Ensure compliance with the safety regulations contained herein, and implement those it deems appropriate so that the Security Document reflects the real situation of the

company at all times.

2) Inform data subjects of the information that is collected from them and for what purposes, and guarantee the exercise of data protection rights to data subjects, through the establishment of an effective, simple and free procedure.
3) Observe the Guiding Principles for the Protection of Personal Data.
4) Ensure that the personal data contained in the databases are relevant, correct, not excessive, and up-to-date for the purposes for which they were collected.
5) Limit the processing of personal data to the fulfilment of the intended purposes. If the Data Controller intends to process the data for a different purpose that is not compatible or analogous to the purposes reported, the consent of the Data Controller will be required again.
6) Make reasonable efforts to limit the period of processing of sensitive data to the minimum necessary.
7) Establish and maintain legal, organizational, technical and specific security measures to protect personal data against damage, loss, alteration, destruction or unauthorized use, access or processing.
8) Maintain confidentiality, directly or through third parties that provide services, with respect to the personal data processed, an obligation that will continue even after the end of their relationship with the owner or, where appropriate, with the Data Controller.

f. SECURITY OFFICER

MSLA ID may delegate the exercise of security functions within the company to the Head of Security, who will be formally assigned the function of control, monitoring and coordination of the security measures reflected in this Document, and must undertake, among others, the actions listed below:

1) Identify the Data Processors, draft the necessary clauses for Access to Data on Behalf of Third Parties and verify that these agreements are signed prior to the start of the provision of services.
2) Keep the company's Information Architecture and Personal Data Flow up to date.
3) Grante, alter, or terminate authorized access to data and resources; A list of users with authorized access to the entity's processing systems must be drawn up and kept up to date, specifying the level of access that each user has.
4) Ensure compliance with incident reporting and management who must keep and update the Virtual Registry of Incidents, classifying them according to their status in: pending, resolved, archived.
5) Ensure that users comply with the declaration of media that make up their Inventory and keep the entity's Virtual Inventory updated.
6) Record the procedures carried out for the recovery of the data, indicating the person who executed the process, the data restored and, if applicable, what data was required

to be recorded manually in the recovery process.

7) Verify the application of the controls established to comply with the established technical, administrative and physical measures.

In order to correctly carry out the multiplicity of entrusted actions, the Security Manager may delegate to whomever he/she deems responsible for the execution of part or all of any of the tasks in his/her charge.

MSLA ID has appointed its Security Officer. Notwithstanding this particular appointment, in the future they may appoint more than one (1) Security Officer to act jointly with the pre-existing one, and/or in any case and whenever they deem it appropriate, revoke the appointment that is now made.

The appointment of one or more Security Officers does not exonerate the Data Controller from liability for non-compliance with the regulations on the protection of personal data.

g. PERSONAL DATA PROTECTION OFFICER

MSLA ID will designate a person, natural or legal entity, or personal data department, who will promote the protection of personal data within the organization.

6.2. ORGANIZATIONAL SECURITY MEASURES

a. PERSONAL DATA SECURITY MANAGEMENT SYSTEM

In order to guarantee the required security conditions in terms of personal data protection, it is vital that the Data Controller is aware of and familiarizes himself with the legal framework in force; commits to providing the resources and direction for effective law enforcement; understand the institutional context in the processing and protection of personal data (organizational, technological, legal, legal, contractual, regulatory, physical, etc.); and clearly determine appropriate organizational roles and responsibilities with sufficient authority and resources to lead and enforce the security policy for the protection of personal data.

Adequacy to the protection of personal data is not satisfied with the drafting of a personal data protection policy, but requires security measures and procedures, so that through a process of continuous improvement, an acceptable level of risk is achieved in the processing of personal information, in accordance with the model and objectives of the organization.

Although Law No. 29733 and its Regulations do not require the implementation of a Personal Data Security Management System (hereinafter, SGSDP) or to follow any standardization standard, it is expressly recommended to adhere to the guidelines outlined by the Data Protection Authority of the Republic of Peru through its Security Directive.

b. PERSONAL DATA PROTECTION POLICY

MSLA ID has developed a documented commitment to respect the principles of the Law, where it determines and discloses its personal data protection policy. MSLA ID's Personal Data Protection Policy is a brief and direct statement, drafted under the scheme and following the design provided by the Personal Data Protection Authority, which demonstrates the institutional commitment and involvement with the protection of personal data in the treatment given to the personal data contained in the personal data banks under its ownership. In order to make it known to the holders of personal data, the Personal Data Protection Policy is hosted on the corporate website.

c. PERSONAL DATA SECURITY DOCUMENT

This Security Document has been drafted according to the types of data being processed, the risk involved, the systems and the way in which they are processed, in order to guarantee the confidentiality, availability and integrity of the information.

The Data Controller will arbitrate the means to communicate to the staff and all collaborators who have access to personal data, the security measures and procedures that are applicable to them, and the due treatment that they must carry out of the personal data of third parties within the exercise of their functions.

This master security document, which sets out the security measures and procedures required for the correct processing of personal data, will be kept up to date, so that it always reflects the company's personal data protection standard. To this end, once the Personal Data Security Document has been implemented and communicated, it is essential that it be reviewed and evaluated periodically.

d. REVIEWS OF SECURITY MEASURES

Every one (01) year, the Security Officer will try to review the Security Document and the Annexes that describe the procedures in force, in order to verify the correct functioning and implementation of the security measures, warn of failures and vulnerabilities and carry out the corresponding updates or other processes that have undergone substantial modifications and do not reliably reflect the processing of personal data of the entity.

For the processing of information, MSLA ID uses the following policies:

- Physical Security Policy-MSLAID
- SDLC Policy and Procedures-MSLAID
- Systems Backup Policy-MSLAID

e. FLOW OF PERSONAL DATA

This section describes the life cycles of the personal data that MSLA ID uses to carry out its business management.

The following is a description of the main flows of personal data that occur in the company, broken down by area:

- WORKER DATA FLOW

  Personal Data Flows that occur in the MSLA ID Employee Personal Data Bank:

  ✓ PERSONNEL SELECTION

  The life cycle of personal data begins with the publication on the various job platforms of advertisements with job offers at MSLA ID, which initiates a process of selecting personnel with a certain profile, according to the needs of the company. Through the portal, personal data is captured. The data comes from those candidates who voluntarily apply and send their CVs to participate in the selection process. Candidates who pass the first selection filter are contacted via email or telephone. The rest of the CVs are rejected and do not add to the database.

  The interview is arranged, at which point the applicant brings to MSLA ID the CV summarized in physical form. A personal interview is taken with HR and an exam to prove their technical aptitudes according to the position applied for. If the candidate is suitable, they are passed on to an interview with Management. If Management approves, you will be asked for your consent for the processing of your sensitive data and you will be required to provide additional personal data.

  The occupational medicine service is outsourced to a medical professional and a clinic where the examinations are performed. Both the doctor and the clinic inform MSLA ID that they make the interested parties sign a consent form.

  The company sends the results to MSLA ID .The doctor receives and keeps the results and the entire report in his custody, and sends to Human Resources only the first page, where the qualification of fit – unfit to carry out the tasks is recorded. If the person is eligible, a file is opened as an employee of the company.

  If the candidate is rejected, the physical file is kept for the current year, in order to participate in future selection processes that fit their profile. After one year, the CVs of rejected candidates are deleted.

- ✓ CONTRACT MANAGEMENT

The life cycle of personal data begins with incorporation as an employee of the company, from the signing of the employment contract. Human Resources opens a file for each employee of MSLA ID. The physical file is scanned, it is registered in the HR folder of the Server. The physical file is archived.

In the event of the termination of the employee, due to resignation or dismissal, the Human Resources area prepares the settlement together with the rest of the termination documentation, signed by the Manager.

- ✓ PAYROLL MANAGEMENT

The Human Resources area is in charge of managing the WORKERS database, payroll and social security contributions, through the premium payroll system whose access is with a password.

To calculate the hours actually worked by each employee, attendance control is used at the company's headquarters – through the SISCOP software.

The information is entered into the aforementioned systems on a monthly basis by the Human Resources area, the accounting area is also given access to the system, and some information is sent by encrypted email, which performs the accounting control of the payroll payment and authorizes the payment, sending the data to the Administration.

All the areas involved use and manage the information according to their roles and responsibilities, and in case they receive information via email, once they have carried out their control and executed the task in their charge, they must delete the respective email. The payroll data is then uploaded to the portal of SUNAT and the Ministry of Labor.

- ✓ OTHER DATA FLOWS

The Workers' personal database is also used for the management of staff training and induction; management of permits, vacations and licenses, management of work insurance, and management of control and compliance with biosecurity protocols for the COVID-19 virus.

In relation to the management of vacations, permits and licenses, they are managed by the Human Resources area, through the SISCOP software system.

To record personnel movements, the Human Resources area has various formats (e.g. vacation letter) that are saved in physical format in the employee's file and recorded in the SISCOP system.

Regarding insurance policies, they manage the coverage, which is sent by the contracted insurance company virtually or physically, and is stored physically in the worker's file. They are also registered in the SISCOP system, in order to keep track of the validity of the policies.

- DATA FLOW FOR IDV SERVICES

  Flows of Personal Data that occur in the Personal Data Bank of Customers and Third-Party Data Banks are detailed into DATA PROCESSING FLOW FOR PROSPECTING AND EHANCEMENT SERVICES of MSLA ID.

- PURCHASING & PAYMENT MANAGEMENT

  The Administration area carries out the management of suppliers, customer management, and collections and payments.

  To manage the requested purchase, within the Personal Data Bank of suppliers, Administration accesses the suppliers folder of the ANT ERP system where the suppliers with whom MSLA ID works are registered.

  Payments are the primary responsibility of the Administration area. Payments are made through the Telebanking application, which is encrypted using an e-token cryptographic device.

  Finally, they make the payroll payment, as reported by Human Resources through the ANT ERP system. Prior to making the payment, Administration requests authorization from Management.

- VIDEO SURVEILLANCE DATA FLOW

  Flow of Personal Data that occurs within the Video Surveillance Personal Data Bank:

  MSLA ID has implemented a closed-circuit surveillance camera (CCTV) for each of its headquarters, with cameras on the outside, inside (production and warehouse) of the company. The images are recorded on a disc, and re-recorded monthly (every 30 days).

  The venues are as follows:

  - ✓ Administrative Office: Paseo de la Castellana 18, Madrid. It has 04 cameras.

f. PRIVACY CULTURE

MSLA ID will arbitrate the means to guarantee the effective knowledge by users of the security policies described herein, the rights and obligations that concern them, as well as inform about any changes that are made to the Personal Data Security Document in the future, whose application will not be retroactive.

To this end, MSLA ID's staff and collaborators will be trained on personal data protection regulations, in order to avoid future data security breaches, as well as breaches due to ignorance of the regulations.

g. PRIVILEGE ASSIGNMENT MATRIX

In order to identify the personnel of MSLA ID who have access to personal data owned by the Data Controller, as well as the access permissions that each agent will be assigned, according to the role and profile they occupy within the company, the Matrix that relates the personal data processing systems with the users who handle such assets is drawn up in this Document.

This Matrix will serve as a guide to delimit access to personal data for MSLA ID employees, and for any agent who has access to personal data. In order to guarantee the adequate protection of personal data, access to the data must be restricted in accordance with the permissions assigned by the Security Manager to each user, in accordance with the position they hold, their functions and the data they use.

Once completed in accordance with the parameters indicated below, the matrix must be periodically reviewed by the Security Manager, in order to keep it up to date, reviewing the criteria for assigning access permissions, purging those users who have ceased to be in the position, and modifying the permissions of users who have changed their activity within MSLA ID and onboarding new users where appropriate.

According to the position and profile that the agent occupies within the company, the access permissions that may be assigned to personal data are:

- ✓ **P: Procurement**
- ✓ **U: Usage**
- ✓ **D: Disclosure**
- ✓ **S: Storage**
- ✓ **B: Blocking**
- ✓ **C: Cancelation**

PRIVILEGE MATRIX PERSONAL DATA BANK						
Permissions that can be assigned to an agent:					P: Procurement	
					U: Use	
					D: Disclosure	
					S: Storage	
					B: Blocking	
					C: Cancelation	
STAFF AUTHORIZED	AREA	x	DP ROLE	x	TREATMENT SYSTEMS	
Names and last names	Management		Security Manager		Server (Local/Cloud)	
	Administration					
	Human Resources		Primary Responsible		Email	
	Marketing					
	Treasury		Responsible		Paper	
	Sales		PDP		SOFTWARE (ERP, SISCOP, ETC)	
	Accounting					

h. TRACEABILITY

Through the use of email accounts, it is possible to identify who had access to personal data and the processing carried out by users. The Controller will use this information to verify the correct use of the assets and the proper behavior of the systems.

i. INCIDENT MANAGEMENT

An incident is understood to be any anomaly that affects or may affect the security and integrity of personal data, systems, computer media and documents (whether automated or not).

It is the obligation of all users to notify the Data Controller and/or the person to whom they have delegated the administration of computer systems, regarding any incident (regardless of its relevance) that occurs in the processing systems and/or in the data stored in them. Such communication must be made as soon as possible, from the moment the incident occurs, or it is certain that it could occur or is known of it, following the procedure established herein.

Here all users must rely on the Incident Management Policy and Procedures-MSLAID.