DATA DISPOSAL AND ANONYMIZATION POLICY

Code: POL-TI-006
Revision: 01
Data: 05/01/2023

WWW.DMSLOG.COM

1. OBJECTIVE

Guide and establish DMS LOGISTICS' corporate guidelines for the proper disposal and anonymization of data.

2. FIELD OF APPLICATION

All employees, service providers and internal and external users of the information owned/custodied by DMS LOGISTICS.

3. REFERENCE DOCUMENTS

This policy applies to all documents that are information assets or not and that are in the possession of DMS LOGISTICS. For reference purposes, the General Data Protection Law (LGPD) - Law 13.709/18 and the ABNT NBR ISO/IEC 27001:2022 were used.

4. RULES PROCEDURES

4.1. Definitions

4.1.1. Applicability

In this document, when there are mentions of attributions and / or responsibilities to DMS LOGISTICS, the scope to be considered will be DMS LOGISTICS and all its Subsidiaries.

4.1.2. Anonimização

Use of reasonable technical means available at the time of processing, through which a data loses the possibility of association, directly or indirectly, with an individual.

4.1.3. Anonymised data

Data relating to the holder that cannot be identified, considering the use of reasonable technical means and available at the time of its treatment.

4.1.4. Data disposal

Process of deleting or deleting a data record without the possibility of reversal or reconstruction of the information.

4.1.5. Personal Data Mapping (ROPA)

Document with the identification of the flow of personal data used in the organization's processes. It contains details about the treatment of this data, including how and from where it is collected, and how it is used, stored,shared and discarded.

4.1.6. General Data Protection Law (LGPD)

Brazilian law regulates the use, protection and transfer of personal data by natural persons or legal entities governed by public or private law.

4.1.6.1. Data Title

Natural person to whom the personal data refers.

4.1.6.2. Controller

Natural or legal person, of public or private law, who is responsible for decisions regarding the processing of personal data.

4.1.6.3. Operator

Natural or legal person, of public or private law, who carries out the processing of personal data and on behalf of the controller.

4.1.6.4. Data Processing

Any operation carried out with personal data, such as those relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

4.1.6.5. National Data Protection Authority (ANPD)

Public administration body responsible for ensuring, implementing and verifying compliance with the LGPD throughout the national territory.

4.1.6.6. Purpose

From the LGPD it will no longer be possible to process personal data for generic or indeterminate purposes. The processing of each personal information must be done for specific, legitimate, explicit and informed purposes.

4.1.7. IT Equipment

Computers, smartphones, laptops, tablets, or any other mobile device that has access to the organization's network and information.

4.1.8. Data Protection Officer (DPO)

He is in charge, the main figure of Personal Data Governance. It is a person appointed by the controller and operator to act as a communication channel between the controller, the data subjects and the ANPD.

Among its attributions are:

• Accept complaints and communications from the holders, provide clarifications and take action;

• Receive communications from the ANPD and take action;

• Guide employees and contractors of the entity regarding the practices to be taken in relation to the protection of personal data;

• Perform other duties determined by the controller or established in complementary standards .

4.2. Acronyms

ROPA – Record of Processing Activities

LGPD – General Data Protection Law

ANPD – National Data Protection Authority

4.3. Data Disposal and Destruction

Disposal is the last phase of the data lifecycle in an organization. It is a practice that helps reduce data storage costs and contributes to a more efficient management of Information Security. In addition, with the arrival of the LGPD, the disposal of data is no longer just a good practice and becomes also a mandatory practice in certain contexts, as is exposed below in this document.

In summary, the disposal of data has as main objectives:

• Be a fundamental part of the management of data storage capacity; • Reduce costs related to data storage;

• Strengthen the guarantee of good Information Security and data governance practices;

• Follow the guidelines of the LGPD for the conditions of processing of personal data, taking into account the rights of the holder guaranteed by the Law.

4.3.1. Criteria for Disposal

In general, there are two reasons to keep data stored in an organization: either it has legal regulatory value, or it generates effective results for the business. Through a process of analysis of the flow of information it is possible to identify in which of these divisions they are. If it is not suitable for any of these categories, the information may be discarded.

To See the data that generate results to the business, it is necessary to have an alignment of the IT area, which is the area responsible for electronic information systems, with the business areas. For this, it is important that the process of maintaining the ROPA, described in the LGPD Governance Policy, is followed, ensuring that the ROPA is always up to date. Thus, data that no longer has use and will no longer be used in the future, can be identified for possible disposal.

For the evaluation of the legal regulatory value of information, it is important to highlight that the standards followed by the organization are not static, but are in constant transformation. Therefore, the IT area must have a continuous process of communication with the legal area so that the criteria for defining the data that needs to be stored and the data that can be discarded are established and updated.

Following these guidelines, DMS LOGISTICS adopts requirements for data disposal , following the data processing processes identified in ROPA. It seeks to ensure that only the necessary data is processed and stored by DMS LOGISTICS,

All Personal data processed by DMS LOGISTICS will be retained for the time necessary to fulfill the purpose for which they were collected, for lawful, specific and informed purposes.

Some data must be stored to comply with legal obligations,such as those of a tax, labor and social security nature. In such cases, the data will be stored until the end of the period stipulated by the legislation.

Others, related to contracts and operations of a commercial and logistical nature, will be stored for the necessary time, following a deadline consistent with market practices and the nature of the treatment.

Personal data that achieves its purpose and storage period will be deleted through the following methods:

Method	Description	Applicable to
Physical destruction	Physical destruction of storage media with the use of specialized choppers, sprayers or incinerators. This method completely destroys the media of all data.	Hard drives, removable disks. CD, CDR, DVD, DVDR. This method is also valid for material in physical support such as printed and the like;
One-way encryption	Use of a one-way hash to encrypt information irretrievably, even if in possession of the encryption key. This method does not affect the media and can be used for selective disposal of information.	Hard drives, removable discs, CDR, DVDR and the like;

This policy sets out the guidelines for deletion, disposal or anonymization of personal data.

4.3.2. LGPD and Data Disposal

Prepare an impact report on the protection of personal data upon request of the ANPD, which shall contain at least:

• Description of the types of data collected;

• Methodology used to collect and ensure the security of information; • Analysis of the controller with respect to measures, safeguards and risk mechanisms adopted.

The ANPD will request, when it deems it necessary, a report of impact on the protection of personal data from the data controller. Therefore, DMS LOGISTICS must be prepared to prepare the report whenever necessary. For this, it is important that the organization is aware of the information that the ANPD may request and that this information is easily available.

To assist in the preparation of the data protection impact report, DMS LOGISTICS will use its model of this report, based on the main guidelines of the LGPD.

4.3.3. Good Practices for Safe Disposal

The procedures for disposing of information deemed safe do not have to be the same for the different classifications of information – for information on the classification of information, see the Information Classification Policy. Thus, the safe disposals for each type of information should be carried out as described below.

• Confidential (NC1) or restricted (NC2): the information must be destroyed so that it is not possible to recover it, regardless of the available means. When the information is located in the partners, the latter should be guided as to the correct form of disposal.

• Internal Information (NC3): the information must be destroyed so that it is not possible to recover it, regardless of the available means;

• Public Information (NC4): there is no restriction on the form for disposal.

It is important to emphasize that there must be a process so that the disposal of data can be documented properly, and the records are made in reliable and secure systems.

4.3.4. IT Systems

At DMS LOGISTICS, the data stored in your IT systems can be hosted on your own on-premises servers or on the cloud servers of partner companies.

For cloud data storage cases, it is especially important that responsibilities over data are shared and well defined between DMS LOGISTICS and the company providing the service. DMS LOGISTICS must require that good information

security and data disposal practices be followed by the partner company, a point that must be reinforced in the contract.

The LGPD, in Article 39, determines that the operator must carry out the treatment according to the instructions provided by the controller. In addition, Article 42 of the Law says that the operator is jointly and severally liable for the damages caused by the processing when it has not followed the lawful instructions of the controller. Therefore, the sharing of responsibilities and the legal requirements in relation to the information security of DMS LOGISTICS towards the partners is fundamental for the secure disposal of data in the context of the LGPD, implying in the relaxation of sanctions in case of violations of the Law.

For data stored on its own local servers, the secure disposal of data is reinforced by compliance with Good Physical Security Practices, which keep servers free from unauthorized access.

4.3.5. IT Equipment and Mobile Storage Media

The disposal of data from IT equipment and storage media should happen in the following hypotheses:

• Exchange of the assignment of an equipment or media between employees of DMS LOGISTICS or third parties;

• Return of the asset once in the possession of an employee or third party to DMS LOGISTICS.

• Return of the asset to the supplier in case of rented equipment; • Mobile storage media devices are no longer needed or damaged. These must be disposed of safely, being necessary to be returned to IT for safe disposal, which will carry out the disposal process in appropriate environments.

In any case, the responsibility for the process of secure disposal of information will be the IT area , leaving the user of the asset responsible for communicating to the IT area any need for secure disposal of unforeseen data.

In critical cases, more extreme techniques should be used for information destruction, including degaussing, overwriting or even physical destruction. For this, equipment and services that make the seg ura deletion of the devices must be used so that no data is retrieved.

4.3.6. Physical Documents

Once the need has been verified or when the disposal of physical documents is convenient for DMS LOGISTICS, subject to the conditions present in this Policy, these documents must be destroyed, without the possibility of reconstruction, before being discarded.

Often, the same record can exist in both electronic and physical format. In such cases, DMS LOGISTICS must define what the official format is so that the unofficial version can be safely discarded.

4.3.7. Data Anonymization

Article 12 of the LGPD establishes that anonymized data will not be considered personal data, except when the anonymization process to which they have been submitted is reversed, using exclusively its own means, or when, with reasonable efforts, it can be reversed.

Therefore, when the LGPD brings the obligation to delete personal data, according to the hypotheses set forth in this document in the item "The LGPD and the disposal of data", and when the data in question are still useful to DMS LOGISTICS, an alternative to deletion may be the anonymization of this data.

In addition, the anonymization of data can also be used as a reinforcement for Information Security in the organization in general. In summary, data anonymization is convenient in the following contexts:

• To avoid damages and sanctions in case of leakage of personal data, if this information is useful for DMS LOGISTICS even in its anonymized forms;

• When, through mandatory exclusion by the LGPD, DMS LOGISTICS deems that the information is still useful in some way for the generation of value in the organization;

• For secure storage, transfer and sharing of personal data.

4.3.8. Good Data Anonymization Practices

One point of attention is that ensuring effective anonymization of data, in a scenario of strong technological evolution, may not be simple. In order for the Law to be fully complied with, therefore, DMS LOGISTICS must evaluate the degree of security that is applied in its anonymization processes.

Given this scenario, it is very likely that, as authorized by the 3rd paragraph of Article 12 of the LGPD, a regulation will be issued providing for the standards and techniques to be used in anonymization processes. Thus, the anonymization of data should be carried out under the following conducts:

• Following the standards and techniques that may be established by the LGPD, thus ensuring alignment and support against the Law;

• Applying techniques that DMS LOGISTICS has evaluated as safe, preferably using state-of-the-art techniques that are constantly updated. The responsibility for the execution, registration, control and effectiveness and evaluation of the processes of anonymization of electronic data should be the IT area of DMS LOGISTICS. Still, the anonymization may be outsourced, being done by an independent company, provided that it certifies that the anonymization will use good practices and will follow any LGPD guidelines in relation to acceptable techniques and standards.

5. REVISION HISTORY

Revision	Data	Description
00	09/02/2023	Issuance of the document.
01	24/02/2023	General review to include new commitments to the environment, employee health and safety, and information security and coding in the document.

6. APPROVAL AND CLASSIFICATION OF INFORMATION

Prepared by:	CyberSecurity Team	
Reviewed by:	Leonardo Sabbadim	
Approved by:	Victor Gonzaga	
Level of Confidentiality:	**X**	**Public Information**
		Internal Information
		Confidential Information
		Confidential Information

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM