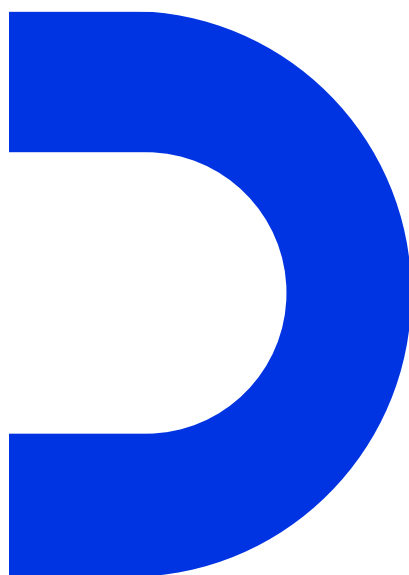




# PRIVACY AND PROTECTION OF PERSONAL DATA

Internal Regulations – Corporate Policies

Date: November 2021

Code: PC-04-5.2-08-202111

## Introduction

Approval of the Global Dominion Access, S.A., (hereinafter "**Dominion**") Privacy and Protection of Personal Data Policy (hereinafter, the "Policy") is yet another milestone in Dominion's steadfast commitment to lawfulness, ethics and professionalism that underpins how it conducts its operations and its corporate culture.

Pursuant to this Policy, Dominion is firmly committed to:

- | Complying with and fully adhering to all current legislation (both nationally and in the countries where it operates).
- | Complying with the principles that govern its Code of Conduct which forms the basis of the Policy set out here.
- | Training and raising awareness of the Obligated Parties (as this term is defined below), as well as stakeholders, of the importance of complying with this Policy.
- | Applying penalties for non-compliance with the provisions set out herein, pursuant to the applicable disciplinary measures.

Using this Policy, Dominion intends to establish the common and general principles and guidelines of conduct that should regulate the protection of personal data, providing a constant guarantee that applicable legislation will be met.

Specifically, the Policy guarantees data protection rights for all physical people who deal with Dominion, guaranteeing respect for the right to honour and privacy when different types of personal data are processed, from different sources and for different purposes, depending on the business activities performed by the company.

## Scope of application

The Policy applies to all employees, managers and directors of all the companies that make up Dominion (hereinafter "**Obligated Parties**").

For the purposes of this Policy, "Dominion" shall also mean all companies which Global Dominion Access, S.A. controls or may control, directly or indirectly, with control being understood to be:

- (i) holding the majority of the voting rights;
- (ii) the right to appoint or remove a majority of members of the Board of Directors; or
- (iii) holding the majority of the voting rights pursuant to eventual agreements made with third parties.

Likewise, all third parties who have dealings with Dominion will also indirectly receive this document and, whenever possible, must be made aware of the underlying principles and values.

## Commitments and principles of conduct

Dominion will scrupulously comply with applicable data protection legislation in the jurisdiction under which the personal data is processed and that determined in accordance with any binding rules or agreements adopted by Dominion.

Dominion will also advocate that the principles set out in this Policy are taken into account:

- (i) in the design and implementation of all procedures involving the processing of personal data;
- (ii) the products and services Dominion offers;
- (iii) in all contracts and obligations they enter into with natural and legal persons; and
- (iv) in the implementation of any systems and platforms that allow Dominion employees or third parties to access personal data and/or the collection or processing of such data.

## Basic principles concerning personal data processing

The principles concerning personal data processing which this Policy is based on are set out below:

### Principles of lawfulness, legality and fairness regarding personal data processing.

Personal data processing shall be lawful, legal and fair, in compliance with applicable legislation. To this regard, personal data must be collected for one or more specific and legitimate purposes, pursuant to applicable law.

When required by applicable law, the data subjects' consent must be obtained before their data is collected.

Also, whenever so required by law, the reasons why personal data is processed must be specified in a clear and detailed manner when it is collected.

In particular, Dominion will not collect or process personal data relating to ethnic or racial origin, political ideology, beliefs, religious or philosophical convictions, life or sexual orientation, union membership, health, or genetic or biometric data aimed at unequivocally identifying a person, unless the collection of such data is necessary, legitimate and required or permitted by applicable law, in which case they will be collected and processed in accordance with the provisions of that law.

### Principle of minimisation

Only personal data that is absolutely necessary for the specific purpose it is being collected or processed for and which is appropriate for the purpose in question will be processed.

## Principle of accuracy

Personal data must be both accurate and up-to-date. If not, it must be deleted or corrected.

## Storage limitation principle

Personal data will not be kept beyond the period necessary to achieve the purpose for which they are processed, except in the cases provided for by law, pursuant to the relevant data retention policy which is established according to Dominion's division and/or jurisdiction.

## Principles of integrity and confidentiality

When personal data is processed, an appropriate security system must be guaranteed, by means of technical or organisational measures, to protect them from any unauthorised or unlawful processing and to prevent them from being lost, destroyed or accidentally damaged.

The personal data that Dominion collects and processes must be kept with the utmost confidentiality and secrecy, and cannot be used for any purposes other than the ones this its collection has been justified and allowed for, and this data cannot be disclosed or transferred to third parties except in those cases permitted by applicable legislation.

## Principle of proactive responsibility

Dominion shall be responsible for observing the principles set out in this Policy and those set out in applicable law and must be able to provide evidence of its compliance whenever applicable law so requires.

Dominion must perform a risk assessment on the processing actions that it carries out to identify the applicable measures to ensure that personal data is processed pursuant to the legal requirements. Whenever legally required, the risks that new products, services or information systems may pose in terms of personal data protection will be assessed in advance and any necessary measures will be taken to eliminate or mitigate them.

Dominion shall keep a record of activities describing how personal data is processed in the context of its activities.

Should an event arise that results in the unintentional or unlawful destruction, loss or alteration of personal data, or the unauthorised disclosure of or access to such data, the internal procedures established to this regard by the management in charge of corporate security at Dominion and those procedures established by the applicable legislation must be adhered to. Such incidents must be documented and measures shall be adopted to resolve and mitigate potential adverse effects for the concerned parties.

In the cases provided for by law, data protection officers shall be designated - according to the Dominion division and/or jurisdiction - in order to ensure that the data protection standards are upheld in Dominion.

## Principles of transparency and information

Personal data shall be processed in a transparent manner in relation to data subjects, with the provision to data subjects of intelligible and accessible information regarding the processing of their data when so required by applicable law.

For purposes of ensuring fair and transparent processing, the Dominion company that is responsible for the processing must inform data subjects whose data are to be collected of the circumstances relating to the processing in accordance with applicable law.

## Acquisition or procurement of personal data

It is forbidden to purchase or obtain personal data from unlawful sources, from sources that do not sufficiently ensure the lawful origin of such data or from sources whose data have been collected or transferred in violation of the law.

## Engagement of data processors

Prior to engaging any service provider that may have access to personal data for which Dominion is responsible, as well as during the effective term of the contractual relationship, Dominion must adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing by the data processor is performed in accordance with applicable law.

## International transfers of data

Any processing of personal data that is subject to European Union regulations and entails a transfer of data outside the European Economic Area must be carried out strictly in compliance with the requirements established by applicable law in the jurisdiction of origin. In addition, Dominion companies located outside the European Union must comply with any requirements for international transfers of personal data that are applicable in their respective jurisdictions.

## Rights of data subjects

Dominion must allow data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability and objection that are applicable in each jurisdiction, establishing for such purpose such internal procedures as may be necessary to at least satisfy the legal requirements applicable in each case.

## Information storage duration

The personal data Dominion processes will be subject to storage duration terms that are specifically established according to the Dominion division and/or jurisdiction.

## Reporting Wrongdoings

All Obligated Parties have a Whistleblowing channel to report any conduct that may involve any wrongdoing or any illegal actions or any actions that go against the Code of Conduct or Policy. For further details regarding the Whistleblowing Channel, consult the [Code of Conduct](#).

## Document sheet

Document table:

|                      |                     |
|----------------------|---------------------|
| Document Type        | Corporate Policy    |
| Document code        | PC-04-5.2-08-202111 |
| Date of the document | November 2021       |

Prepared by:

| Name or role                 | Remarks | Date          |
|------------------------------|---------|---------------|
| Risk & Compliance Department |         | November 2021 |
|                              |         |               |
|                              |         |               |
|                              |         |               |

REVISED BY:

| Name or role                   | Remarks / Approved by | Date |
|--------------------------------|-----------------------|------|
| Audit and Compliance Committee |                       |      |
|                                |                       |      |
|                                |                       |      |
|                                |                       |      |

## Table of Editions:

| Edition | Date | Description |
|---------|------|-------------|
|         |      |             |
|         |      |             |
|         |      |             |
|         |      |             |