General Data Protection Policy

1. Compliance Policy

a) Cox operates in the market with full respect for individual rights relating to the protection of honour and privacy, in each of the jurisdictions in which it operates.

b) Employees are not authorized to carry out, authorize or tolerate conduct that violates Data Protection regulations, honor and privacy, or Cox's policy in this regard.

c) Employees must take reasonable steps to ensure that other employees under their authority and/or responsibility are aware of and comply with this policy.

d) There is zero tolerance for non-compliance; any employee who fails to comply with the provisions of this Program may be subject to sanctions, including dismissal.

e) The Company will ensure that all employees have access to information and understanding of the provisions of this Program and to the necessary legal advice.

f) There is a Reporting Channel where all employees can report any behaviour that may be considered illegal or questionable, for investigation and resolution.

g) This policy is a general summary. The administrative body has specifically empowered the Data Protection Officer to be responsible for the design, implementation and execution of the policy and the management of risks arising from Data Protection.

2. Applicable regulations

It is the set of laws and other positive regulations, agreements and practices voluntarily assumed and internal regulations of the company. It includes, among others and in a merely enunciative manner, the following that has been taken into account in a principal manner for the implementation of this Program without prejudice to the necessary contrast with each local legislation of those jurisdictions in which Cox operates that must be carried out in a preventive manner:

- ✓ The Treaty on European Union and Directive 95/46
- ✓ EU Data Protection Regulation (as amended on 12 March 2014 by the European Parliament on a proposal from the Committee on Civil Liberties, Justice and Home Affairs (LIBE)).
- ✓ Organic Law 15/1999 on the Protection of Personal Data
- ✓ Regulation of the previous one, according to Royal Decree 1720/2007, both of the Kingdom of Spain
- ✓ Mexico's Data Protection Act

- ✓ Data Protection Act of the United Kingdom.

- ✓ The Global Electronic Commerce, Video Privacy Protection Act and the Fair Credit Reporting Act of the USA.

3. Development

Most countries and jurisdictions have mandatory regulations or guidelines on market practices relating to a business's holding and use of personal data about individuals.

The purpose of these regulations is to guarantee and protect public freedoms and the fundamental rights of natural persons, and especially their honour and personal privacy.

For the purposes of this Policy, "data" or "personal data" means any numerical, alphabetical, graphic, photographic, audio-visual or any other type of information concerning natural persons who can be identified or identifiable by said data.

A "file", "data file" or "database" refers to any collection of personal data organized in a way that allows access to the data using certain criteria.

It therefore applies regardless of the medium (paper lists, computer databases), the means of processing (manual or automatic) and the data itself (alphabetic such as names, numeric such as passport numbers or images, such as surveillance cameras at office entrances).

For example:

- Data relating to training, evaluations, payrolls and personnel administration.
- Selection and evaluation of candidates.
- Data relating to clients, suppliers and/or collaborators.
- Project management and control data.
- Data relating to administration, finance and accounting.
- Recording images by security cameras at the entrances or own facilities
- Database of employee photographs.

Files for exclusively personal or domestic use limited to the private life of individuals are excluded.

Each society is responsible for

1) Organize your data files (access, deregistration/registration, etc.).
2) Register or notify, if required, the files before the supervising government authority, as well as the quality of the data, and obtain the consent of the affected party.
3) Notify the existence of the database and, where applicable, its content, to the government authority (national/federal or state/regional) responsible for supervising the data protection law.
4) Maintenance of the applicable security measures for the protection of the file.
5) Implementation of technical and organizational measures for file management.
6) The data is strictly confidential.

7) All media, programs, cameras or any means of data capture must have a legal notice incorporated regarding the data they capture and warnings to the user and their rights of access to it.

Tasks related to file processing such as:

1. Declaration and updating of common files between companies in the same group or subgroup.
2. Maintaining security measures at the appropriate level (low, medium, high) through privacy impact assessment analysis

It is also advisable in all cases, and in some jurisdictions, it may be mandatory, to have a Data Protection Officer (DPO) in the company for legally provided cases. The DPO will supervise the implementation and use of data protection measures and policies, acting as the interlocutor between the authorities and the company and assisting the data controller in more specialized matters.

4. International Transfers

The transfer of data from one country to another is particularly sensitive, even if it is carried out between subsidiary companies of the same group. Prior legal and technical advice on this matter is essential for each company.

Contracts under which international transfers of data to a third country that does not have an adequate level of protection (understood as established in the EU Directive) are made possible must contain the obligation to inform public authorities of data access.

5. Individual rights of the person whose data is processed

Depending on each national legislation, the person whose data is obtained, stored and processed has the inalienable right to:

- Access to your data
- Rectification if your data is incorrect
- Cancellation (deletion, erasure and forgetting) of your data once the relationship has ended.
- Opposition

These rights guarantee that a natural person can exercise control over his or her personal data. These are rights whose exercise is highly personal and non-waivable.

The exercise of these rights must be carried out through simple and free means made available by the person responsible for the file and which are subject to a deadline, so it is necessary to establish procedures for their satisfaction.

If the claimant believes that his or her rights have not been addressed in the manner and time frame, he or she may seek legal protection from the government agency supervising them.

- **Right of Access**
  The right of access is the right of the affected party to obtain information on whether their own personal data are being processed, the purpose of the processing that, if applicable, is being carried out, as well as the information available on the origin of said data and the communications made or planned thereof.

- **Right of Rectification:**
  Right of the affected party to have data that is found to be inaccurate or incomplete modified.

- **Right of Cancellation:**
  Right of the affected party to have data that is found to be inadequate or excessive deleted.

- **Right of Objection:**
  The right of the affected party to not have their personal data processed or to have it ceased (in cases where consent is not necessary for processing), when the files are for commercial prospecting, or for the purpose of making decisions regarding the interested party and based solely on the automated processing of their data.

6. List of Conducts Contrary to Regulations or Risks

- Failure to register or notify the files before the supervisory government authority if required
- Possession or collection of data without consent or with opposition from the affected party
- Lack of security measures to control the quality of data and its processing.
- Transfer of data without consent.
- Handling of personal data
- Disclosure or publication of data out of context.
- Creation of user profiles based on previously obtained data.

If there is evidence, proof or suspicion that a Cox employee, competitor, client or supplier is violating competition laws, this must be reported in accordance with the provisions of the Whistleblowing Channel.

7. The required and prohibited conduct for employees are:

7.1. Required Conduct:

- Organize your data files (access, deregistration/registration, etc.).

- Register or notify, if required, the files before the supervising government authority, as well as the quality of the data, and obtain the consent of the affected party.
- Notify the existence of the database and, where applicable, its content, to the government authority (national/federal or state/regional) responsible for supervising the data protection law.
- Maintenance of the applicable security measures for the protection of the file.
- Implementation of technical and organizational measures for file management.
- The data is strictly confidential.

7.2. Prohibited Conduct

- Possession or collection of data without consent or with opposition from the affected party
- Transfer of data without consent.
- Handling of personal data
- Disclosure or publication of data out of context.
- Creation of user profiles based on previously obtained data.

If there is evidence, proof or suspicion that a Cox employee, competitor, client or supplier is violating competition laws, this must be reported in accordance with the Whistleblowing Channel section.

The **whistleblower channel** The Cox Reporting Procedure is common to all five companies and to companies controlled by Cox. The confidentiality of the whistleblower is guaranteed, as is the transparency and objectivity of the reporting procedure and its resolution. The Reporting Procedure regulates this process in detail.

Entry into force : This document enters into force upon approval by the Board of Directors and will remain in force until it is updated, revised or repealed. The current version, revised in September, 29, 2024, is the current one, approved by the Board of Directors on November, 21, 2024. This policy must be kept up to date and may be revised annually, and on an extraordinary basis, whenever there are changes in the strategic objectives or applicable legislation, with the Compliance Director submitting a proposal for modification to the Compliance Committee, and from there to the Board of Directors.

Cox ABG Cox		
Policy	• General Data Protection	
Responsible	• Board of Directors	
Area	• Corporate – Regulatory Compliance	
Version Control	Date	Changes
1	September 29, 2024 / Nov 21, 2024	majv