

Privacy and Personal Data Protection Policy

cca LAW FIRM

A. INTRODUCTION

Cruz, Salinas, Mayer & Associados, Sociedade de Advogados, SP, RL, with NIPC (legal entity number) 504.046.799 and having its registered office at Edifício Diogo Cão, Doca de Alcântara Norte, 1350-352 Lisboa (CCA) is a law firm with offices in Lisbon and Oporto, whose activity is guided by high standards of responsibility and professional ethics, governed by the principles of integrity, transparency, honesty, loyalty, thoroughness and good faith.

'Innovation that Transforms Realities, Solutions that Impact People' is our purpose, but we can only do this with the above principles in mind and based on our values: quality, commitment, innovation, flexibility and diversity.

At CCA, we believe that the way we work, develop and relate to each other mirrors our culture and DNA, and that this should be aligned with our purpose, values and principles.

CCA is committed to protecting the Personal Data entrusted to it on a daily basis by CCA Members, suppliers, Clients, partner entities and other stakeholders, and has therefore implemented the necessary technical and organisational measures to ensure an adequate level of security.

Within the scope of its activity, CCA has access to personal data of CCA Members, as well as access to personal data of Clients, suppliers and partner entities, and their staff, the processing of which is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or the General Data Protection Regulation ("GDPR"), Law No. 58/2019, of 8 August, which implements the GDPR in the Portuguese legal system and other applicable legislation.

CCA believes that the personal data of CCA Members, Clients and Third Parties is of the utmost importance and is therefore committed to protecting the personal data entrusted to it.

This Policy is intended to provide information on how we collect, process and even store personal data, and to establish compliance in terms of internal practices and define procedures for the operation or operations carried out on personal data or on sets of personal data, by automated or non-automated means, such as collection, registration, organisation, structuring, storage, adaptation or amendment, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure or destruction.

We invite everyone who is subject to this Policy to read it and familiarise themselves with its content, remembering that failure to comply with the rules set out here exposes CCA to fines of up to twenty million Euros (€20,000,000) or 4% of its annual worldwide turnover for the previous

financial year, whichever is higher.

B. PRIVACY AND PERSONAL DATA PROTECTION POLICY

CHAPTER I

GENERAL PROVISIONS

1. PURPOSE AND SCOPE

All CCA Members are bound by this Privacy and Personal Data Protection Policy (also referred to as "Policy") and, as such, must comply with it, as well as with any other related policies in force at CCA.

The competent CCA bodies or departments should alert all those mentioned in the previous paragraph to the existence of the Policy.

This Policy is part of a set of policies and codes and should be read together with these documents, in particular the Code of Ethics and Conduct. This policy is an integral part of CCA's Annual Security Plan, together with the other internal data protection policies in force, and should be reviewed at the same time, whenever justified.

For the purposes of this Policy, and in addition to those specifically mentioned herein, the following terms and expressions shall have the meaning specified below, when beginning with a capital letter, in the singular or in the plural:

CCA: Cruz, Salinas, Mayer & Associados, Sociedade de Advogados, SP, RL, legal person number 504046799, with registered office at Edifício Diogo Cão, Doca de Alcântara Norte, 1350-352 Lisbon;

Code of Ethics and Conduct: a set of principles that govern CCA's activity and rules of ethical and deontological nature to be complied with by CCA Members, including members of administrative and management bodies, in their relations with CCA Members themselves, with Clients, Suppliers and other stakeholders. It is also aimed at third parties, hired by or acting on behalf of CCA, in cases where CCA may be held responsible for their actions. It is available at www.cca.law;

Clients: people and organisations engaging CCA's services;

Personal Data: any information relating to a natural person (the Data Subject) which identifies them or makes them identifiable. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data recipient: a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not (this is the case, for example, when CCA, in compliance with the law, sends personal data to the Social Security or Tax Authorities for the purpose of complying with its reporting and tax obligations);

DPO or Data Protection Officer of the CCA: person appointed by CCA to perform the duties of Data Protection Officer;

Staff: any worker, employee, service provider and/or any person appointed by a Client, supplier or partner entity to deal with CCA;

CCA Members: All lawyers, partners, of counsels, service providers and all employees within the CCA structure. This also includes summer trainees;

Pseudonymisation: the processing of personal data in such a manner that the data can no longer be attributed to a specific person without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational measures to ensure that the data are not attributed to an identified or identifiable person;

Controller: the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Processor: a natural or legal person which processes personal data on behalf of the Controller (for example, accountancy firms that process the personal data of CCA Members are deemed to be Processors for all intents and purposes);

Third Parties: natural persons in respect of whom CCA has access to personal data as a result of the services it provides to Clients (e.g. data of representatives or employees of Parties with whom it has a commercial relationship);

Data processing: means any operation or set of operations performed with personal data, whether or not in a manual, logical or automated manner. Operations such as collection, recording, organisation, structuring, storing, adaptation, alteration, retrieval, consultation, use, transmission, making available, combination, erasure or destruction are always data processing operations (for example, CCA processes personal data whenever it processes salaries and fees);

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

CHAPTER II

GENERAL PRINCIPLES

ALIGNMENT

CCA processes the personal data of CCA Members on a daily basis, as well as the access to the personal data of Clients, Suppliers and Partner entities, and their Staff.

We understand that the privacy and respect for the personal data of those who work with CCA must come first and we are fully committed to ensuring that the trust placed in us is never compromised.

In addition, we are aware of the importance of data protection for CCA Members, Clients, Suppliers and partner entities, as well as the role and responsibility we assume when we undertake to process the personal data they entrust to us.

This concern cuts across the entire organisation and extends to all areas of activity.

Personal data protection is integral to our design process and is embedded by default in all our services.

We believe that in order to achieve an environment that truly protects personal data, we must continue to promote the implementation of these sensitivities in our internal systems, processes and procedures.

This Policy underscores the importance we place on personal data protection and highlights the depth of our commitment to safeguarding it.

PRIVACY BY DESIGN AND BY DEFAULT

Within the framework of its processes, CCA implements internal guidelines and applies measures that comply, in particular, with the principles of data protection by design and by default of its services, for example, by only collecting data that is truly necessary to meet the purpose of its collection.

These measures are designed to minimize risks to Data Subjects arising from data processing activities.

CHAPTER III

PERSONAL DATA

DATA RELATING TO CCA MEMBERS

Personal data is provided and collected in the context of the relationships established between CCA and CCA Members. The processing of this data is essential for CCA to be able to carry out its daily activities.

OTHER SOURCES

In compliance with its obligations or in the course of the recruitment process, CCA may collect information from other entities.

PURPOSES OF PROCESSING

CCA may process personal data for different purposes. For each purpose, we must have a specific legal basis that justifies the processing. While this Policy provides an overview of the various purposes for processing your personal data, we will always specify the exact legal basis for processing your personal data for a specific purpose, at the time of collection. We will only process personal data that is essential to fulfill the stated purposes.

The processing of your personal data may be necessary for the defence of the data subject's vital interests, e.g., in the event of an accident or accident on CCA premises, we may need to access and process personal data in order to locate and contact a relative or friend.

CONSENT

Whenever data processing is based on consent, the following rules must be complied with:

When provided in a written document, the consent must be presented in a clear, accessible, and legible manner;

The document will present the different purposes for which the data is intended in an individualised manner and clearly distinguished from each other;

The data subject shall have the right to withdraw consent at any time, in accordance with the provisions hereof.

INFORMATION

Personal data will always be processed:

Lawfully and in compliance with the principles of good faith, loyalty and transparency;

For specific, express and legitimate purposes, and personal data will not be further processed in ways that are incompatible with the original purposes for collection;

Adequately, in a relevant manner and not excessively in relation to the purposes for which it is collected and subsequently processed;

Accurately and up-to-date;

Using appropriate technical and organizational measures to ensure its protection;

The data will be stored in such a way as to allow the identification of the data subjects only as long as necessary for the purposes of collection or further processing.

Whenever CCA collects data, it must state the following at the time of collection:

The identification of the Controller;

The purposes for which the data is processed;

The reason for the processing, namely CCA's legitimate interest if applicable;

The categories of personal data processed;

The recipients or categories of recipients of the data, in particular the existence of data transfers outside the European Economic Area (EEA) and the specific safeguards implemented;

Whether the provision of data is compulsory or optional;

Any consequences of not providing the data;

The methods available for data subjects to exercise their rights under data protection legislation;

The period for which the data will be stored, or if that is not possible, the criteria used to determine that period.

SERVICE PROVIDERS

When personal data processing is carried out by a service provider, CCA ensures that it will only engage providers that demonstrate sufficient guarantees for implementing appropriate technical and organizational measures to comply with current data protection legislation.

CCA will ensure that any engagement of service providers that process personal data of CCA Members takes place under a written contract binding both CCA and the service provider, specifically outlining the essential standards defined in this Policy.

The provider may only engage another service provider with CCA's explicit prior written consent.

The service provider's refusal to comply with the same obligations regarding data protection, as mandated by the applicable legislation and binding CCA, will result in:

Renegotiation of the contract; or,

Termination of the contract.

Breaches of contractual obligations will result in the service provider being held civilly and criminally liable.

PROVISION OF DATA TO THIRD PARTIES

We may from time to time share personal data with Third Parties.

This will be made soley for the purposes expressly defined herein, and CCA undertakes to guarantee the confidentiality of your personal data.

This may take place, in particular, in the following circumstances:

To our service providers such as insurance companies, telecoms companies, auditors, travel agencies, hotels, car rental companies, lawyers or banks;

To public and private organisations, in the context of public tenders for which CCA is bidding and service proposals;

Public and private organisations for presentations, promotions and events.

TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA ('EEA').

CCA does not transfer your personal data outside the European Economic Area ('EEA').

STORAGE PERIOD

CCA stores personal data in a way that allows you to be identified, only for the period necessary for the purposes for which the data was collected.

The specific period for which your personal data is stored will, however, depend on the specific relationship you have with us and the relevant data. For example, we will keep your data for a period of five years after you stop working with CCA because, in certain circumstances, we are required to do so by law. We are also required to keep your access records for the purposes of labour legislation. Here are some examples of the storage periods we apply to your personal data:

RELEVANT DATA	STORAGE PERIOD
Health data for assessing working capacity (Law No. 102/2009)	5 and 40 years after termination of contract
Video surveillance data (Article 13, DL No. 35/2004, of 21 February)	30 days after the images are taken
Tax retention periods (CIRC: Article 130 - tax documentation file)	10 years after termination of contract
Retention periods under CIVA (Article 52 CIVA)	10 years after termination of contract
Recording working time (Article 202 Labour Code)	5 years after termination of contract
Performance assessment	1 year after termination of contract
Salary processing	1 year after termination of contract
Benefits management (bonuses and remuneration in kind)	1 year after termination of contract
Seizure management and payment of union dues	For as long as they are necessary for the purpose in question
Management of disciplinary proceedings	1 year after termination of contract
Managing accidents at work	5 years after termination of contract
Labour claims (Article 337 Labour Code)	1 year from the day after the employment contract ended.

SECURITY OF PROCESSING

CCA has implemented the appropriate technical and organisational measures to guarantee a level of security that is commensurate with the risk, considering the state of the art, implementation costs, and the nature, scope, context, and purposes of the processing involved.

These measures include, in particular, and as appropriate:

Pseudonymisation and encryption of personal data;

Maintaining permanent confidentiality, integrity and availability of information;

Maintaining the level of resistance of the systems and services associated with the processing of personal data;

The ability to restore availability and access to data in a timely manner in the event of incidents, both physical and technical;

Measures that ensure regular analysis and evaluation of the effectiveness of the technical and organisational measures implemented;

We employ a range of technical and organisational security measures to protect your information, including firewalls and access controls, which we review periodically. Additionally, we ensure that CCA Members receive appropriate training in security and data protection.

PERSONAL DATA BREACH

In the event of a personal data breach, CCA notifies the competent authorities within seventy-two (72) hours of the occurrence, under the terms established in the Personal Data Breach Response Policy available on the CCA Intranet.

Any person who becomes aware of a situation of Personal Data Breach must report it, without undue delay, to CCA's DPO via the following e-mail address dpo@cca.law in the terms expressly provided for in the 'Personal Data Breach Policy'.

Personal Data Breaches must be recorded and documented as expressly provided for in the Personal Data Breach Response Policy.

EXERCISING RIGHTS

As Data Subjects, individuals have the right to access, rectify, restrict, object to, portability and erasure of personal data.

CCA guarantees that the exercise of these rights will have no associated costs.

CCA will respond to all contacts regarding the exercise of rights in a timely and reasonable manner, but no later than one month.

In certain circumstances, CCA may not satisfy the request when it considers it to be unfounded, or when the request conflicts with our legal obligations, always providing justification. This does not preclude the data subject from lodging a complaint with the Portuguese Data Protection Commission.

RIGHT OF ACCESS

The Data Subject is entitled to know what specific data is processed by CCA.

The information will be provided in writing and may cover the following information:

Data type;

Manner of use;

Recipient of the sharing of personal data;

Personal data storage period;

Rights of the Data Subject;

How the data was obtained and the organisation supplying it, when it has not been provided directly;

The existence of automated decisions, or profiling based on personal data.

1. RIGHT TO RECTIFICATION

17.1. CCA relies on the accuracy and currency of the data provided, and the Data Subject has the right to rectify it.

18. RIGHT TO OBJECT

18.1. The Data Subject covered by this Policy has the right to object, at any time, to the processing of their personal data. In this case, and provided the necessary legal requirements are met, CCA shall stop processing the personal data.

19. RIGHT TO ERASURE (Right to be forgotten)

19.1 The Data Subject has the right to ask CCA to erase their personal information, in particular when:

19.1.1 The personal data is no longer necessary for the purpose for which it was collected or processed;

19.1.2 The Data Subject has withdrawn consent, in cases where CCA is processing personal data on the basis of that consent;

19.1.3 The Data Subject has exercised their right to object to the processing of their personal data;

19.1.4 The personal data has been unlawfully processed;

19.1.5 Personal data must be erased in order to comply with a legal obligation applicable to CCA;

19.2 Despite the above, CCA is not required to erase the data when:

i. The exercise of freedom of expression and information is at stake;

ii. It is required by law to process the data covered by the request; or

iii. For reasons related to the declaration, exercise or defence of a right in legal proceedings.

20. RIGHT TO PORTABILITY

20.1. The Data Subject has the right to ask CCA to transfer the personal data to a third party of their choice or to hand over the same data in a structured, commonly used and machine-readable format, without prejudice to the provisions of the following paragraph.

20.2. The right to portability only exists when:

- The data is being processed on the basis of consent; or
- In the performance of a contract, or
- Data processing is carried out by automated means.

21. EXERCISING RIGHTS

21.1. To exercise any of the above rights, the Data Subject must send a written request to the following e-mail address dop@cca.law.

CHAPTER IV

PROCESSING OF SPECIAL CATEGORIES OF DATA

(SENSITIVE DATA)

22. SPECIAL CATEGORIES OF DATA

22.1. In the course of its business activity and service delivery, CCA may access and process special categories of data of CCA Members, as well as Clients, suppliers and partner

entities. For all intents and purposes, sensitive data or 'special categories of data' shall include any and all information:

a) That reveals racial or ethnic origin; or,

b) Relating to political opinions, religious or philosophical beliefs; or,

c) Relating to trade union membership; or,

d) Genetic data; or,

e) Biometric data; or,

f) Health data; or,

g) Data relating to sexual life; or,

h) Data relating to the Data Subject's sexual orientation.

23. LEGAL BASIS AND PURPOSES

23.1. CCA will process 'special categories of data' solely for one or more specific purposes and in accordance with the law, namely:

23.1.1. When it has obtained express consent for the processing of such personal data, where applicable; or,

23.1.2. For the purposes of complying with obligations and exercising specific rights of CCA, in particular with regard to labour legislation, for example for the purposes of preventive or occupational medicine;

23.1.3. For the purpose of contract performance;

23.1.4. To satisfy legitimate interests, such as monitoring via video surveillance cameras.

24. ENHANCED DUTY OF SECRECY

24.1. Without prejudice to the inherent duty of confidentiality in legal practice, to which CCA Members are subject, they are bound to maintain absolute secrecy concerning any information they access, which may include 'special categories of data'.

24.2. Those in possession of information that they know, or should reasonably know, contains sensitive data must refrain from using such information for any purposes other than those explicitly instructed by CCA.

25. PRACTICES AND RULES OF CONDUCT

25.1. CCA Members who, for whatever reason, become aware of the existence of information relating to 'special categories of data' which are readily available or unduly accessible must, as soon as possible, give written notice thereof to the relevant Management/Heads/Department, as well as CCA's Data Protection Officer.

25.2. Such notice must include:

25.2.1. Information characteristics;

25.2.2. Location where the information can be accessed;

25.2.3. If possible, when did the information become available;

25.3. If the information containing sensitive data is intended to be known by a group of people in the context of a project, operation or service, the team leader will inform the group of the sensitivity of the type of information they will be receiving and must provide the following details in writing to the respective Management/Heads, as well as to CCA's Data Protection Officer:

25.3.1. Identity of all the people who know the information;

25.3.2. Information characteristics;

25.3.3. Deadline by which this information will be available.

26. INFORMATION SECURITY (SENSITIVE DATA)

26.1. Without prejudice to the appropriate technical and organisational measures in place to protect personal data as mandated by law, CCA Members who possess information containing sensitive data must in any case, and without prejudice to the contractual confidentiality obligations to:

26.1.1. Limit access to information to specific individuals on a need-to-know basis for the effective performance of their duties;

26.1.2. Refrain from commenting on it in order to avoid revealing, directly or indirectly, its existence or content;

26.1.3. Use it solely for its legitimate purpose;

26.1.4. Comply with the measures that allow adequate control of access to information and the documents and other media in which it is included;

26.2. Require the prior execution of a non-disclosure agreement before disclosing sensitive information to Third Parties, when necessary.

27. RESTRICTIONS ON USE

27.1. Those possessing information that they know or, under the circumstances, should know contains data related to 'special categories of data' must refrain from disclosing it to Third Parties.

27.2. CCA Members who become aware of access to sensitive data by an individual who is not subject to any obligations in this respect must give written notice to CCA's DPO as soon as possible. Such notice shall detail:

a) How they became aware of the breach;

b) The identity of all individuals who are not bound by any obligations in this regard but are aware of the information;

c) Information characteristics;

d) Date on which the individual who is not subject to any obligation in this respect had access to the information.

27.3. Should CCA Members become aware of any breach of the information security rules, they must report this breach in writing to CCA's DPO with the details listed in the preceding paragraph.

27.4. Any breach of these restrictions will result in appropriate disciplinary and criminal action.

CHAPTER V

SPECIFIC PRINCIPLES

28. CCA MEMBERS

28.1. The processing of personal data relating to CCA Members will be carried out in accordance with the applicable law.

28.2. CCA does not employ any systems to monitor CCA Members, in particular, no systems are in place to control communications, monitor Internet usage, or mechanisms that in any way allow the automatic assessment of the performance of those within the CCA structure.

28.3. The processing of data related to CCA Members is based on:

28.3.1. The management of the labour relationship, particularly in terms of human resources management and salary processing;

28.3.2. Managing relationships with service providers, including lawyers, of counsels and others, for the purposes of human resources management and payment of fees;

28.4. An additional Privacy Statement must be signed, particularly with regard to sensitive data, under the terms of the legislation in force, without prejudice to the contracts concluded between CCA and CCA Members, where applicable, including a clause relating to the processing of personal data.

29. SUPPLIERS AND PARTNERS

29.1. The relationship with suppliers and partners must always be based on a contractual instrument that complies with the rules and principles set out in this Policy.

29.2. When the supply and/or partnership involves any access to personal data, there must be specific clauses governing the way the supplier and/or partner accesses the data.

29.3. The supplier and/or partner may act, for the purposes of the relationship, as a processor or a data controller:

29.3.1. If the supplier and/or partner acts as a processor, the latter must state and accept by that any operation conducted is always on behalf of CCA;

29.3.2. If the supplier and/or partner acts as a data controller itself, the latter must explicitly ensure compliance with the applicable security rules as well as the data protection principles outlined in the legislation, namely the legal basis for processing, limitation, type and exercise of the rights of the Data Subjects.

29.4. The supplier and/or partner's refusal to accept its obligations regarding data protection, as required by the standards to which CCA is subject or as mandated by applicable legislation, shall result in:

i. Renegotiation of the contract; or,

ii. Termination of the contract.

29.5. Breaches of contractual obligations will result in the supplier and/or partner being held civilly and criminally liable.

30. CLIENTS

30.1. Operations involving the personal data of Clients, their clients or Third Parties must always be based on a contractual instrument.

31. CONTRACTUAL PRINCIPLES

31.1. Operations involving the processing of personal data on behalf of CCA, or in which CCA carries out the processing on behalf of Clients, must adhere to at least the following requirements:

31.1.1. Processing operations, namely transfers and/or communications of personal data, must be carried out under documented instructions only;

31.1.2. A non-disclosure agreement must be in place;

31.1.3. Adequate measures to ensure a level of security appropriate to the risk of processing and the personal data to be processed must be ensured and preferably defined;

31.1.4. The methods for assisting the controller in fulfilling its obligation to respond to requests from data subjects in order to exercise their rights;

31.1.5. Upon termination of the processing or the contractual relationship, personal data is erased or returned, and any existing copies are deleted, in accordance with the legal requirements to which CCA or the Client are subject;

31.1.6. No other processor is engaged unless the controller has previously given specific or general authorisation in writing;

31.1.7. The scope, duration, nature and purpose(s) of the processing;

31.1.8. The categories of personal data concerned;

31.1.9. The categories of CCA Members concerned;

31.1.10. CCA's obligations and rights and,

31.1.11. The obligations and guarantees provided by the processor.

CHAPTER VI

SECURITY MEASURES

32. PHYSICAL SECURITY MEASURES

32.1. Physical security measures are implemented through security policies for all information users who have access to personal data.

32.2. Physical security measures include, without limitation:

32.2.1. Controlling access to buildings, in particular through the use of access cards;

32.2.2. Entrance registers, monitoring of doors and restricted access rooms;

32.2.3. The existence of security personnel on site, as well as alarms;

32.2.4. All individuals without authorised access to controlled areas must enter and be accompanied by someone with approved access to the controlled area.

32.2.5. Access rights to controlled areas are revalidated in full every year and revoked upon the termination of the contract.

32.2.6. The facilities where personal data is stored must be protected against environmental factors and power failures.

33. SECURITY SYSTEMS

33.1. To ensure the safety of individuals, facilities, and property, CCA has implemented video surveillance systems (CCTV). Areas under surveillance are clearly marked on-site.

34. DIGITAL SECURITY MEASURES

34.1. CCA has implemented security policies that incorporate specific software for these purposes, namely:

a) Antivirus, firewall and data prevention loss software;

b) Limitation on sharing unauthenticated files;

c) Limiting the use of Peer-to-Peer applications;

d) Database encryption software;

e) User account passwords;

34.2. Data transfer is carried out solely via a network and secure connection.

34.3. Internal access controls are defined by the Human Resources Department

34.4. With regard to privileged access, only expressly authorised users can request access.

34.5. A periodic review is conducted based on received instructions to verify which users holding credentials are still authorized by CCA, along with an annual revalidation to ensure that access rights align with the current user base.

34.6. Any exceptions identified during the revalidation process are promptly addressed, and the user's access is revoked upon the termination of the contract.

34.7. Verification passwords must always be implemented in accordance with the following requirements:

a) Minimum 8 characters long;

b) They must contain a combination of alphabetic and non-alphabetic characters (number, punctuation marks or special characters) or a combination of at least two types of non-alphabetic characters;

c) They must not contain user identification as part of the password; and,

d) They should not be generic/trivial.

CHAPTER VII

FINAL PROVISIONS

35. KNOWING AND IMPLEMENTING THIS POLICY

35.1. **Knowledge, compliance and collaboration**

CCA is responsible for implementing the necessary mechanisms to disseminate this Policy internally, ensuring that all CCA Members are aware of its content, and any changes thereto.

An up-to-date version of this Policy must be made available internally, in an easily accessible place on CCA's intranet.

35.2. **Doubts**

Any doubts regarding the application or interpretation of this Policy should be promptly directed to CCA's Data Protection Officer (identified in TABLE 1 below), through the appropriate channels. In the event of any doubts, individuals should refrain from any behaviour until these doubts are clarified.

Unfamiliarity with or misinterpretation of the contents of this document shall not be considered a valid excuse for non-compliance.

36. POLICY AND THE LAW

36.1. In the event of any inconsistency between the Privacy and Data Protection Policy and the applicable legislation, the latter shall prevail.

REQUESTS FOR INFORMATION

37.1 Any request for information on the interpretation or content of this Policy should be made in writing to the following e-mail address dpo@cca.law.

34. MONITORING AND CONTROL OF THE POLICY

38.1. The implementation and compliance with this Policy will be supervised by the DPO.

38.2. This Policy will be periodically reviewed and/or modified by CCA, specifically by the DPO, who may engage the services of professionals specialised in crime prevention and regulatory compliance matters whenever:

- There are significant changes in the organisation, the control structure or the activity carried out by the entity that make this advisable;
- Legal changes arise that make this advisable;
- Relevant violations of its provisions occur, making this advisable; and
- Any other situation occurs that justifies a review.

38.3. It is the duty of CCA Members to periodically consult the updated version of this Policy.

39. APPROVAL AND DISSEMINATION

39.1. This Policy, as well as any revisions and amendments thereto, shall be approved by CCA's Executive Committee.

39.2. Once approved, this Policy will be disseminated internally and will come into force immediately. Updates to the Policy contained in this document will be valid from the date of approval, without prejudice to subsequent changes.

39.3. The latest version of this Policy will be available at all times on CCA's intranet and must be made available to third parties, suppliers, Clients and partner organisations, including their staff, who deal with CCA and have access to CCA's IT and Technical Resources.

TABLE 1 – 'CCA's Data Protection Officer'

Year	Name	Contact
2024	Martim Bouza Serrano	dpo@cca.law
2023	Martim Bouza Serrano	dpo@cca.law

Version History

Version	Approval	Date
1.1	Executive Committee	September 2024
1.0	Executive Committee	December 2023