Bankinter Group
Code of Professional Ethics

The Bank's Board of Directors has approved the Bankinter Group's Code of Professional Ethics (Code of Ethics or CPE), which constitutes the set of basic action principles and practices of professional conduct of all employees and persons working for the Bankinter Group.

The Code of Ethics forms part of Bankinter's people management policy, which gives top priority to the following values:

- Promoting talent and intellectual capital
- Ensuring a free, creative and motivating working environment
- Transparency and reliability of the Bank's information, including financial information

Principles which, together with the commitment to quality, good corporate governance, social responsibility, compliance with applicable laws and regulations and the creation of value in the long term for shareholders, employees, the company, clients and society as a whole, define our organisation's ideology.

The Bankinter Group is also firmly committed to the principles of Corporate Social Responsibility as a framework for its policies and actions towards employees, clients, suppliers, shareholders and all stakeholder groups with which it has relations, together with the implementation of systems for the prevention and investigation of any criminal acts that might affect the Group.

The significance taken on by these values in the Bank makes it advisable to delimit their scope, ensure that they are conformed to throughout the Organisation and establish the rules of conduct guiding the professional activity of all employees.
The Code of Ethics is organised into the following Articles:

Article 1. Scope of Application

Article 2. General Principles

Article 3. Confidentiality

Article 4. IT Programs and Systems

Article 5. Professional Loyalty

Article 6. Employees' Personal Transactions

Article 7. Governing Bodies

Appendix I - Code of Professional Ethics Monitoring Committee

**Article 1. Scope of Application**

1.1 Compliance with the Code of Ethics is mandatory for all employees of Bankinter and persons affected by it, without prejudice to the special duties applying to employees subject to the Bankinter Group's Internal Regulations on Conduct in the Securities Market and the Codes of Conduct applying to certain areas or departments of the Bank or Group companies.

The Code of Ethics applies to the employees of Bankinter, S.A. and of subsidiary companies of Bankinter, agents, scholarship holders, interns, persons on subcontract and, in general, all such persons who work for or provide services to the Bank, as well as the family members and related persons referred to in section 6.4 of this Code if applicable. The Code also applies to Bankinter personnel who have left their posts upon retirement or early retirement, to the extent that they continue to provide any kind of service to the Bank or companies in its Group. The term "employees" comprises, for the sole purposes of this Code, all the persons indicated.

In the case of persons not linked to the Bank by any of the relationships mentioned in the preceding paragraph, the Bank's Regulatory Compliance Unit (RCU) will determine which obligations of the Code of Ethics are not applicable to them. In the case of persons on subcontract who provide services to the Bank through a company, such company must expressly guarantee its
personnel's compliance with the principles of the Code in the corresponding contract.

1.2 The control of the application of the Code of Ethics is the responsibility of the RCU, without prejudice to the functions assigned to the Code of Ethics Monitoring Committee and other areas of the Bank. The RCU will periodically inform the Board of Directors' Audit and Compliance Committee of the status of compliance with the Code of Ethics.

1.3 The communications and requests for authorisation provided for in this Code of Ethics, as well as any queries relating to the contents thereof, shall be sent to the head of the corresponding Unit (or the person designated by the head for the purpose) in accordance with the following list (in which is indicated the corresponding Article and section of this Code):

- Denouncement of serious irregularities: Chairman of the Audit and Compliance Committee.
- Denouncement of breaches of the Code (Article 1.4): RCU.
- Monitoring and supervision of the rules for the Internal Control System for Financial Information (ICSFI) and the internal rules on matters relating to securities markets, in accordance with the criteria and procedures established for the purpose (Article 2.6): Internal Audit Division and RCU respectively.
- Denouncements relating to activities that might lead to criminal liability for the Bankinter Group (Article 2.7): Code of Ethics Monitoring Committee.
- Relations with the media (Article 3.1.3): External Communication.
- Participation in courses, classes, seminars and similar forums (Article 3.1.4): People Management/External Communication.
- Matters concerning IT programs and systems (Article 4): People Management.
- Authorisation to contract with the Bank, information, consultations and decisions on questions of conflict of interest, dedication, incompatibility and relations with clients and suppliers (Article 5): RCU.
– Responses to official requirements (Article 5.4): National Administrative Centre, under the supervision of the Legal Advice Department in cases handled by means of the urgent procedure.

– Client certificates (Article 5.4): National Administrative Centre, once the request has been input in the corresponding database (GEMA). In case of doubt, the National Administrative Centre will consult with the Central Legal Advice Department on who is to issue the certificate.

– Duty of information and consultations on employees' transactions involving securities, credit or financial risk (Article 6): RCU.

All communications, notifications and authorisations referred to in this Code may be carried out by means of e-mail. The RCU will archive documents signed by employees in manuscript or electronic form.

1.4 Cooperation in Compliance with the Code

No employee shall be obliged to follow orders or instructions that are contrary to the Law or to the principles contained in the Code of Ethics. If a situation of this kind should arise, the employee can turn to the RCU or use the confidential denouncement procedure.

Article 2. General Principles

Professional ethics constitute, together with good corporate governance, transparency of information and corporate social responsibility, one of the pillars of Bankinter, and as such it is highlighted among the Principles of Corporate Culture of the Bank approved by the Board and published for the whole Group to take note of them.

Bankinter's corporate values require all employees to conform to the most exacting standards of ethics and professional responsibility. In particular, employees directly involved with the markets, with highly sensitive information, with data processing, with suppliers and in dealing directly with clients. The Bank's ethics find expression among other things in compliance with applicable legislation in force and with the Company's internal rules, respect for confidentiality, truthfulness in its relations with clients, and sincere cooperation with the legal, tax and administrative authorities.

To this end, the Bankinter Group will make available to employees such means as may be necessary for them to become familiar with and understand
the legislation applicable to them so that they can perform their professional duties properly, together with such training as may be necessary to ensure correct regulatory compliance, offering to this end training plans on the protocols put in place in the Group, *inter alia*, to detect and prevent the commission of wrongful acts in its activity.

### 2.1 Principle of Non-discrimination and Equal Opportunity

The Bankinter Group respects the principle of non-discrimination on the grounds of race, gender, ideology, nationality, religion, sexual orientation or any other personal, physical, mental or social circumstances of its employees and will promote equality of opportunity for everyone including gender equality, hiring of non-Spanish employees and hiring of disabled individuals.

The Bankinter Group rejects any manifestation of violence or physical, sexual, psychological or moral harassment in the workplace, as well as any offensive or abusive conduct generating an intimidating environment with regard to employees' personal rights.

The Bankinter Group also rejects discrimination in the workplace that is contrary to the fundamental rights of the people working there.

### 2.2 Work-life Balance

The Bankinter Group respects the personal and family lives of its employees and will promote policies that facilitate the best balance between these and their work responsibilities.

### 2.3 Right to Privacy

The Bankinter Group respects its employees' right to privacy, including everything relating to personal data, medical data and financial data in the legally established terms.

The Bankinter Group respects the personal communications of its employees via the Internet and any other means of communication.

Bankinter Group employees undertake to responsibly use the means of communication and, in general, any other resources that the Bankinter Group makes available to them.
The Bankinter Group undertakes not to disclose individual data of employees except with their consent or when obliged to do so by legal, administrative or judicial order.

Bankinter Group employees who in the course of their duties access personal data of other Group employees are obliged to keep them confidential and not to use them for any purpose other than those relating to their work, the foregoing in accordance with the legislation on personal data protection.

2.4 Health and Safety at Work

The Bankinter Group promotes a policy of health and safety at work, and will adopt the preventive measures established in current applicable law and others that may be established in the future. In particular, employees must follow and comply with the preventive measures established by the Bankinter Group in respect of the Prevention of Occupational Hazards, reporting any hazardous situation of which they become aware to their immediate superiors.

2.5 Selection, Evaluation and Professional Development

The Bankinter Group maintains the most rigorous and objective selection policy, focusing solely on candidates' academic, personal and professional merit and on the Group's requirements.

The annual performance evaluation is an open, non-hierarchical process. The climate of opinion among the workforce is sounded systematically. Training of all employees is one of the Bank's strategic investments. Remuneration tied to targets and performance is implemented throughout the Bank. Specific measures are established to ensure that the talents of the highest-potential employees flourish and are valued. The Bank facilitates telecommuting and flexibility in the performance of duties.

It provides incentives for the careers of the youngest employees, helping their talents to flourish and be recognised, and to this end a permanent process of job rotation is maintained, based on a system of continuous training, learning and renewal.

2.6 Transparency of Information

The Bankinter Group is committed to providing its clients and shareholders with precise, truthful and comprehensible information on its transactions,
commissions and procedures for dealing with complaints and resolving incidents.

Group financial information will be drawn up reliably and rigorously, reflecting all such transactions, facts and events as may be necessary in accordance with applicable laws and regulations.

The Bankinter Group undertakes to comply with the applicable regulations in respect of financial information, and with the Recommendations on the Internal Control System for Financial Information (ICSFI) drawn up by the Internal Control Working Group set up on the recommendation of the CNMV (Comisión Nacional del Mercado de Valores, the Spanish securities and exchange commission) and published in June 2010.

2.7 Guarantees of Principles

Any employee having reasonable indications of a breach of any of the principles of this Code of Ethics or the commission of any act in conflict with the law or the rules of conduct of the Code can report it using the confidential denouncement procedure that has been established.

Article 3. Confidentiality:

3.1 Information on the Bank

3.1.1 Any kind of information on the Bank (reports, accounts, balance sheets, objectives, etc.) is of a confidential nature and is subject to professional secrecy, and the contents thereof may not be made available to clients or third parties except with the Bank's explicit authorisation or pursuant to a legal requirement.

3.1.2 Information of a confidential nature includes information on employees' personal particulars, such as that relating to their remuneration, evaluations and health questionnaires, in accordance with the provisions of Article 2.3 above.

3.1.3 Relations of the Bank and of its employees with the media are reserved to the External Communication and Corporate Reputation Division.

Any telephone call, request for information, questionnaire or the like coming from any media organisation must be sent by the employee receiving it to this Department. Employees must seek prior authorisation of the Department before contacting any media organisation for any professional reason.
3.1.4 The participation of employees as teachers, lecturers, presenters, organisers or moderators in courses, classes, conferences, seminars and similar forums will require the prior authorisation of People Management and notification of the event to External Communication. Authorisation will be deemed to have been given if it has not been declined after three business days. In any such participation, which must not affect the employee's dedication to the Bank, the employee shall avoid making any statements or giving any opinions that might compromise the image, interests or confidential information of the Bank, its clients or third parties. Those persons or areas that by reason of their function maintain habitual contact with external forums are exempted from the requirement for authorisation provided in this section. The RCU will maintain a record of the authorisations given and the areas or persons exempted.

3.1.5 The same criteria, except for the requirement for prior authorisation, will apply to employees' participation in social networks, chat-rooms and community forums and other Internet pages and sites, if they express opinions or make comments relating to the Group.

3.2 Information on Clients and Employees

- Information on client transactions and positions is in any case of a confidential nature and must be treated with complete reserve; it must not be used for any purpose other than those inherent in the employee's work or for any purpose unrelated to the Group, nor may it be made available to third parties except in the case of legal requirement.

- The employee's duty of secrecy governs relations with other clients and with third parties, as well as with other employees of the Bank, unless there are professional reasons justifying the communication of the information within the legal limits.

- The viewing of accounts and positions of employees of any level by other employees of the Bank whose function and position do not necessitate access to such accounts constitutes an irregular practice.

3.3 Information on Competitors and Institutions

- Relations with employees, shareholders and clients of other credit institutions shall be conducted with the greatest discretion, without disclosing confidential information of the Bank, its employees or clients or performing any action that could be considered to constitute unlawful or unfair competition.
Employees are obliged to safeguard the confidentiality of any kind of reserved or sensitive information of other companies, institutions or competitors to which they may have access by reason of their responsibilities.

The Bankinter Group rejects the incorporation of any kind of information or physical or electronic documentation of a reserved or confidential nature belonging to another competing institution or company that has been obtained without its consent.

Employees' attitude towards other credit institutions and competitors in general, and towards the authorities and public bodies, must be one of respect and consideration, without making comments or analysis, divulging information or spreading rumours that could damage the image of the sector, the competition or the institutions.

3.4 Protection of Personal Data

The gathering, use, computer processing and commercial treatment of data of a personal nature on clients or any natural third person must be carried out in such a way as to guarantee their right to privacy and compliance with legislation on the protection of personal data and on services of the information society.

Only employees duly authorised by virtue of their duties may gain access, and then only insofar as proves absolutely necessary, to data of a personal nature on employees as required to meet the Bank's tax law, labour law and other legal obligations.

Employees expressly authorise the inclusion of their personal data in the Bank's files, including the data needed to calculate tax retentions, insurance offered or covered by the Bank, all those deriving from the handling of their employment with the Bank and those affecting their relations as clients. They also authorise the transfer of their data to other Group companies for processing for any of the same purposes.

In no case may personal data of clients or employees be processed for purposes other than those legally or contractually provided.

3.5 Extent of Duties of Confidentiality

The duties of confidentiality referred to in this Article shall subsist indefinitely, even after the worker's employment with the Bank has come to
an end. Upon leaving the Bank's employment no worker may take away any kind of information or documentation of the Bank or acquired by the worker in his or her capacity as an employee of the Bank, including that which is in the files of his or her computer terminal, nor may he or she provide or use such information in the interest of another entity or company.

**Article 4. IT Programs and Systems**

**4.1 Rights to the Programs and Systems**

- The Bank owns the property and rights to use and operate the IT programs and systems, hardware, manuals, videos, projects, studies, reports and other works and rights created, developed, perfected or used by its employees in their work or based on the Bank’s IT facilities.

- Employees must adhere to the principle of strict confidentiality in respect of the characteristics of the rights, licences, programs, systems and technological know-how in general the ownership of or operating or usage rights to which correspond to the Bank.

- Employees must not operate, reproduce, replicate or relinquish the Bank’s IT systems and applications for purposes other than those of the Bank, regardless of whether such activity is remunerated or not, and even if such activity is carried out using any system, medium or IT application of the Bank outside the employee's working hours.

- Employees must refrain from using any kind of IT materials without first having ensured that Bankinter Group has acquired the corresponding rights and/or licences. In particular the use of images, texts and drawings in advertising and communications of the Bankinter Group must be approved in advance by the Marketing and Channels department.

**4.2 Criteria for Use of Programs and Systems**

- The use of the IT hardware, systems and programs that the Bank makes available to its employees for their work, including the Internet access and operating facility, must be in accordance with principles of security and efficiency, avoiding any abuse, action or IT function that is contrary to the Bank's instructions or needs.

- Employees may not install or use programs or applications in the computers that the Bank makes available to them if the use of such programs or applications is illegal or may cause damage to the systems or to the image or interests of the Bank, its clients or third parties.
Employees must not use the IT facilities made available to them by the Bank for illicit ends or for any other purpose that might damage the image or interests of the Bank, its clients or third parties, affect the service and dedication of the employee or endanger the functioning of the Bank's IT resources.

Employees must not make use of the Bank's communication media, such as forums, web pages, etc., to express contents, ideas or opinions or give information on political or other contents not related to the Bank's activity, except for messages of a labour-related, humanitarian, cultural or social type which are neutral from the ideological or political point of view and the exceptions provide for by law.

The use of the facilities referred to may be controlled by the Bank, respecting personal privacy in accordance with the law, providing the Bank's IT systems are concerned, irrespective of whether such use takes place in the Bank or by means of telecommuting or any other kind of access.

All employees are responsible for blocking or disconnecting their terminal when they leave the workstation. In the event of absence or termination of employment the Bank may cancel the employee's access rights to its IT systems.

The Bank may access information stored or recorded by employees on servers, media or systems belonging to the Bank where it has good reason to do so.

4.3 Security Protocols

Employees must conform to the security, control, access and usage measures established by the Bank and the personal and non-transferable use of the security codes within the user profiles and access and usage facilities assigned by the Bank to each employee.

Making a personal access system or code available to another employee or to a third party is a practice contrary to the basic principles of security in the use of IT resources.

Compliance with the security protocols established by the Bank and the principles set out on the Bank's Intranet is mandatory.

4.4 Questions
For any consultation, further information or queries about the matters dealt with in this section, employees should first approach People Management.

**Article 5. Professional Loyalty**

**5.1 Conflicts of Interest**

- Employees must never abuse the Bank's trust or take advantage of working for it to their own benefit or that of family members or related third parties.

Employees must not use for their own ends or obtain benefit from the Bank's assets, means and resources. They must not obtain financial or other advantages, such as business opportunities arising from relations with suppliers, either their own or unrelated to their activity, or receive remuneration in money or in kind or access to financing of any kind. In short, they may not take advantage of relations with the Bank's clients or suppliers for their own benefit or that of related third parties, as established hereunder in Article 5.3.

- Nor must employees take advantage of their position in the Bank to obtain, for themselves or for related persons, financial advantages deriving from transactions relating to the Company or of which they may have knowledge as a result of their working for the Bank when the investment was offered to the Company or the Company had an interest in it, nor take advantage of business opportunities of which they have knowledge as a result of their work, unless the Bank has first declined them. Notwithstanding the foregoing, participation by employees in transactions in which the Bank has an interest or in which the Bank actually participates directly must in any case be authorised in advance. A request for permission to participate, indicating the basic characteristics of the investment envisaged, must be sent to the RCU for them to process further. Until such time as explicit authorisation is received from the Bank, the investments referred to may not be carried out.

- Employees must refrain from interfering in or influencing the approval of credit facilities and other transactions or decisions in which they, their family members or the related persons referred to in Article 6.4 of this Code of Ethics have any personal interest. When any of these circumstances pertains, the employee concerned may not participate in meetings of the Risk Committee or in any other meeting in which approval of the transaction is reported or decided, nor may (s)he approach the employees participating in such meetings with the intent to influence the
decision, nor be involved in the signing, execution, control or renewal of the transaction.

- Employees must obtain prior authorisation from the Bank (Regulatory Compliance Unit) in order to:
  
  - Contract or take part in contracting supplies or services to the Bank with natural or legal persons in which they have any direct or indirect interest.
  
  - Acquire, lease or use assets or rights of the Bank.
  
  - Sell their assets or rights to the Bank.
  
  - In general, maintain any business relations with the Bank or carry out transactions unrelated to their employment with the Bank.
  
  - An employee having an interest in any of the transactions referred to in the foregoing paragraph must also refrain from taking part in or influencing the Bank's decision.
  
  - At the Bank's request, employees must provide information on any possible conflicts of interest with the Bank that might affect them because of their personal, family or professional relations, their personal assets or any other well-grounded reason. This information will be treated as confidential and for the exclusive purpose of complying with the Code of Ethics.

In case of doubt as to the possible existence of a conflict of interest, the employee shall consult the RCU.

### 5.2 Dedication and Incompatibility

- Employees must devote all the professional capacity and personal effort necessary to the performance of the duties assigned them by the Bank.

- They must not carry on activities, whether remunerated or not, that might jeopardise the interests or the image of the Bank or affect the independence, impartiality and professional dedication of the employee.

- Membership of or relations or cooperation with political parties or other associations with public ends, and contributions or services to them, must be in a personal capacity, without involving the Bank in any way.
Employees must provide such information as may be requested by the Bank, through People Management or the RCU, on any remunerated activities not expressly authorised in advance, including education and training, that they carry on outside the Bank.

Before accepting or performing any remunerated activity or work outside the Bank, particularly where such activity might clash with the Bank's interests, employees must consult the RCU and People Management or the competent higher body.

Employees are forbidden to perform professional activities, whether paid or unpaid, for other credit institutions or in general companies carrying on activities in competition with those of the Bankinter Group.

5.3 Relations with Customers and Suppliers

Any kind of interference or influence by clients, suppliers or third parties that might affect employees' impartiality and professional objectivity must be avoided. This obligation particularly affects employees that have to take decisions on contracting supplies and services and those that decide on the financial conditions for client transactions.

Employees are prohibited from receiving any kind of remuneration or financing from customers or suppliers of the Bank and in general accepting any kind of remuneration other than from the Bank for services deriving from their work in the Bank.

It is contrary to professional ethics for employees to accept any kind of personal benefit, gifts, invitations, favours or other compensation from clients, suppliers or any other third party. Attendance of social events and invitations to business lunches, seminars and other kinds of training activities that have been previously authorised by the head of the department and the various channels of authorisation provided in this Code shall not be considered personal benefit.

Gifts of a promotional nature or small courtesy gifts may also be accepted, although they must be distributed or raffled among the employees of the organisation or department to which the recipient belongs, except for well-grounded exceptions authorised by the manager of the corresponding department or organisation. The recipient of the courtesy or promotional gift must inform the hierarchical head of the department, who will carry out the distribution by raffle.

In no case may cash be accepted.
– In case of doubt, employees must consult the RCU first.

– The contracting of external supplies and services and relations with suppliers in general, including those relating to the areas of IT systems and services and premises management, must be carried out using transparent procedures that conform to principles of advertising and competition. Any commission, discount or commercial advantage offered to the Bank to the detriment of third parties must be rejected, or passed on as reduced cost or increased revenue for the Bank.

– In their dealings with clients, employees must avoid exclusive relations that tie certain clients to a single employee, make clients' relations with other employees difficult or hamper their free use of the remote banking systems.

– Commercial relations with clients must be governed by principles of maximum quality and transparency of prices and other conditions.

– Clients must be duly informed of the offers of products and services and the risks attaching to them, and special care must be taken to offer clients only products or services that are suited to their characteristics and needs, promoting financial education, ensuring that indebtedness is reasonable and treating clients equitably.

– Employees must convey information truthfully, completely and comprehensibly, and must never knowingly provide incorrect or imprecise information that may lead the recipient into error. All documentation to be used by the client must be drawn up clearly and transparently.

– Employees must avoid any conduct in advertising, marketing and sales that might constitute deception, lack of relevant information, abuse or price manipulation.

– Similarly, employees must refrain from entering into contracts or carrying out transactions that are not expressly included in the Bank's catalogue of products and services or by means of forms of contract or clauses that are different from those authorised by the Bank.

– Incidents and customer complaints must be channelled exclusively through the customer service departments established by the Bank throughout the organisation.
– Employees of the Bank must not act as holders of powers of attorney or representatives of clients, or carry out banking transactions through any distribution channel in the name of clients or using their personal codes. In the case of accounts of family members, employees may act as the holder of power of attorney or mandate for direct family members and related persons (those referred to in Article 6.4 of this Code of Ethics).

– All banking transactions must be correctly formalised and posted to the accounts. In their dealings with clients, employees must in any case apply the best banking practices and standards of transparency, information and protection, as well as the rights accorded to clients by the legislation on the protection of personal data, services of the information society and other applicable provisions.

– Customer service does not justify the payment or receipt of compensation, payments into unrecorded funds or any other practices that differ from those authorised by the Bank. Cash differences must be duly explained in the manner determined by the Bank. Clients' correspondence may be held in offices and centres only provisionally and for special reasons.

– Special attention must be given to complying with the obligations imposed by the legislation on the prevention of money laundering and the financing of terrorism: identify all clients, refrain from carrying out transactions when there is evidence or there are indications that they are linked to money laundering and/or the financing of terrorism, report suspicious transactions to the Anti-Money Laundering (AML) Unit and do not reveal to the client or to third parties the control and investigation actions being taken and cooperate fully with the AML Unit and the public authorities.

– Employees must reject any kind of offer aimed at inducing them to refrain from complying with any of the obligations in respect of the Prevention of Money Laundering and the Financing of Terrorism that are applicable to them, immediately reporting such a circumstance to the AML Unit and the competent authorities.

– Employees are obliged to attend specific training courses relating to the Prevention of Money Laundering and the Financing of Terrorism.

5.4 Relations with Public Bodies

– Judicial requests for information and embargo and/or blocking of client positions received from judicial bodies, government bodies or any other public bodies must always be sent to the National Administrative Centre to be answered in accordance with the provisions of the applicable internal
Circulars. In no case shall an employee answer the requests referred to, which must always be dealt with centrally.

- The issue of certificates and balance and position approvals for clients must be requested by entering the request in the corresponding database (GEMA), and they will be prepared by the National Administrative Centre in accordance with the centralised procedure established by the Bank. In no case may an employee proceed to issue the documents referred to bypassing the procedure described.

- Employees must cooperate loyally through the Audit Division, the AML Unit, the Legal Advice Department, the Administrative Centre or the corresponding area of the Bank, with the judicial, administrative, tax and supervisory authorities in the terms established in the applicable internal circulars, with a view to providing said authorities with a complete and appropriate response within the timeframes established in the circulars referred to.

- Employees, in their capacity as such, shall refrain from offering gifts to authorities, bodies and government offices, political parties and institutions in general, as well as from making contributions for the Bank's account to the entities indicated or to any other entities.

- Relations with investors and financial analysts shall be conducted exclusively through the Financial Information and Investor Relations Division. Relations with the media must be channelled exclusively through the External Communication, Social Action, Corporate Reputation and Brand Division.

- Due to its importance for the reputation of the company and the possibility of the Group itself being held criminally liable, any non-compliance with this section which an employee becomes aware of must be reported through the established channels.

**Article 6. Employees' Personal Transactions**

**6.1 Transactions with Negotiable Securities**

Without prejudice to the special duties of employees subject to the Bankinter Group's Internal Regulations on Conduct in the Securities Market (IRC), employees of the Bank may buy and sell Bankinter shares and other securities for their own account, with the exception of the transactions in securities and financial instruments set out hereunder.
a) Those that interfere with or affect employees' work, activity or dedication to the Bank or the duties imposed on them by legislation currently in force and by this Code.

b) Those carried out on the basis of insider information or significant information obtained from the Bank or from its clients, suppliers or shareholders. This includes all confidential information, whether of a general nature or relating to Bankinter's shares or to any particular negotiable securities or financial instruments, the publication of which could appreciably influence the price of said securities in the market.

In particular, employees with access to insider information shall refrain from carrying out any of the following acts, whether on their own behalf or on that of third parties, directly or indirectly: (i) preparing or carrying out any kind of transaction with the negotiable securities or financial instruments which the information relates to, (ii) communicating said information to third parties, except in the normal performance of their work or position or (iii) recommending a third party to buy or sell negotiable securities or financial instruments or to have another party buy or sell them based on said information. These prohibitions apply to any employee in possession of insider information where the employee knows or should have known that the information is of this nature.

c) Transactions carried out on the basis of the *quid pro quo*, guarantees or intermediation of clients or suppliers of the Bank (except for the intermediation of investment services companies).

Transactions carried out on the basis of credit or overdraft must conform to the provisions of section 6.2 hereunder.

The Bank, through the RCU, may ask employees to inform it of their securities transactions, particularly any transactions that may prove to be other than for ordinary investment or hedging purposes, such as any intra-day sales and purchases, the buying and selling of foreign currency and contracting of derivative products.

In case of doubt as to whether a given transaction is of a speculative nature or a given item of information is privileged or significant, or regarding the interpretation of this section, the employee must consult the RCU in advance. Employees subject to the Bankinter Group's Internal Regulations on Conduct in the Securities Market (IRC) must comply with the obligations laid down in the IRC, as well as with those contained in this Article.

6.2 Banking Transactions
Employees' financing transactions shall be subject to the provisions set forth in the People Management Manual, including credit risks, off-balance sheet risks and other financial risks.

Financing transactions or other transactions involving financial risk with employees, family members of or persons related to employees (as defined in section 6.4 hereunder) must in any case be authorised explicitly and in advance by the Bank.

The terms of deposit or intermediation transactions with employees, family members and related persons will be those applying in accordance with the Bank's internal rules or those habitually practised in the market for clients.

6.3 Expenses for the Bank's Account

Expenses incurred by employees on account of the Bank must be strictly related to the employment activity and supported by documentary evidence in accordance with the provisions of the People Management Manual.

6.4 Family Members and Related Persons

The obligations set out in this Article 6 extend to the following related persons of employees:

- The spouse, unless legally separated.
- The employee's de facto stable partner, unless legally separated.
- The employee's parents and grandparents.
- Children who are dependent minors, or adult children economically dependent on the employee.
- Other family members or, in general, other persons when the transaction is carried out with the involvement, handling or advice of the employee.
- Companies in which the employee has a significant direct or indirect holding conferring control to him or her, meaning holding the majority of voting rights in the company, majority control of the Board of Directors or executive management of the company.
– Persons acting as the holders of powers of attorney or mandates or as the trustees of the employee, his or her family members or controlled companies, or doing so in concert with any of the foregoing.

Allowing or failing to disclose the existence of transactions carried out by the related persons referred to which may contravene the rules contained in this Code of Ethics is a breach of the employee's duty of loyalty to the Bank.

Article 7. Governing Bodies

Without prejudice to the functions proper to the Regulatory Compliance Unit, People Management, Audit Division and other areas of the Bank, a special procedure has been established for sanctioning breaches of this Code. This procedure is contained in Appendix I.

APPENDIX I: PROCEDURE FOR SANCTIONING BREACHES OF THE CODE OF PROFESSIONAL ETHICS

For sanctioning breaches of the Code of Professional Ethics, the Bank has established a Code of Professional Ethics Monitoring Committee, which is empowered to analyse and resolve possible breaches of the Code.

The competent area for handling and resolving cases relating to other breaches of employment conditions is the People Management unit.

This procedure shall be valid for examining and analysing both the facts relating to employees' alleged disloyalty or fraud and those giving rise to their fraud or professional negligence constituting a breach of the Code of Professional Ethics, the Internal Regulations on Conduct in the Securities Market or other internal rules of the Bank in the field of professional ethics and regulatory compliance. The same procedure may also be applied to reviewing actions, detecting, preventing and denouncing crimes, and taking appropriate measures with regard to agents of the Bank, as well as other persons covered by the Code of Professional Ethics and/or the Internal Regulations on Conduct in the Securities Markets.

The imposition of sanctions on General Managers or the like, Organisation Managers and Managers of Central Services Divisions or equivalent, falls
outside the jurisdiction of the Committee. These cases will be dealt with by the CEO, who, in the case of General Managers or the like, shall first consult the Audit and Compliance Committee, and in the remaining cases may consult and must in any case inform said Committee about the resolutions passed.

**Structure**

The Code of Ethics Monitoring Committee (hereinafter the "Committee"), at the proposal of the CEO, shall be made up of such persons as the Audit and Compliance Committee considers appropriate at any given time.

The Chairman or the CEO of the Bank may alter the structure of the Monitoring Committee, and may take part in its meetings whenever they see fit.

Where agenda items affect employees of subsidiary companies of the Group, the head of the company concerned will be invited to take part in the Committee meeting with voice but no vote. Where breaches in areas of the Bank or Group companies not represented on the Committee are concerned, the head of that area or company must be consulted before the Committee deliberates and decides.

The Audit and Compliance Committee will be informed of the appointments and retirements of members of the Committee.

The Committee shall be chaired by the Chairman or the CEO whenever they attend its meetings.

The members of the Committee may delegate to one of the other persons forming it.

The Committee's decisions shall be taken by majority vote of its members. An absolute majority shall be required for the passing of resolutions to dismiss an employee or suspend an employee without sanction.

Meetings may be held remotely, by electronic or telephonic means.

**Start of the Process: Preliminary Phase**

The process of sanctioning conduct can be set in train by any member of the Committee having access to information relating to possible breaches of the obligations imposed by the internal rules previously referred to.

The indications of such conduct will in any case be investigated and analysed by the Internal Audit Division, which will have overall responsibility for
gathering all the data and information necessary for the Monitoring Committee to evaluate, although it is free to request the assistance of People Management or other areas of the Group.

Once this area considers that it has sufficient information on the case, and in any case within the time limits established by rules currently in force on the prescription of the breaches, it will call a meeting of the Committee, attaching a report summarising the results of its investigation. The Chairman of the Committee will add to the report a proposed classification of any alleged sanctionable offences as well as a proposal for sanctions. This proposal shall serve solely as a starting point for the Committee's deliberations and shall in no case bind the final decision.

Committee meetings may also be called by the Chairman or by the CEO.

**Deliberation and Decision Phase**

Once a Committee meeting has been called it shall proceed to deliberate either in a face-to-face meeting or remotely. The imposition of sanctions and the management measures complementing them shall in any case conform to the provisions of labour legislation and, if applicable, to the internal guidelines laid down by the Committee itself or by the Audit and Compliance Committee. If the employee whose actions are submitted for decision by the Committee belongs to the Department or Division of one of the members of the Committee, that member may take part in the debate and express his opinion on the decision to be taken, but must abstain from voting.

If the Committee considers that the decision is significant because of the persons affected, the complexity or far-reaching implications of the matter or its value as a precedent, it must send the decision in the form of a proposal, before officially informing the employee or employees affected, to the CEO and to the Secretary of the Audit and Compliance Committee with a copy to its Chairman, by e-mail, with the particulars relating to the case and the decision made by the Committee.

The CEO, who may first consult the Audit and Compliance Committee or its Chairman, will adopt the corresponding resolution.

The CEO, the Secretary of the Audit Committee or the Head of Internal Audit will inform the Audit and Compliance Committee in the next meeting of cases that are especially significant, whether for quantitative or qualitative reasons, and of the decisions made on them.

The Audit and Compliance Committee may issue binding instructions to the Committee on (i) the general policies of judgement followed by the
Committee in the cases reported, for possible rectification or modification in future cases, (ii) rectification of decisions taken, in exceptional cases (iii) the contents of the set of measures applied by the Committee, (iv) any other substantial or procedural matter it sees fit to mention to the Committee. Compliance with these instructions will be controlled by the CEO and the Audit Division.

The People Management and Knowledge Area will take charge of formalising, communicating and executing the decisions made by the Committee.