



1833

BANCO
CARREGOSA

Privacy Policy

October-2022

V. 1

< This page intentionally left blank >

Table of Contents

I.	Versions Index.....	v
II.	Properties.....	v
III.	Legislative sources and reference documents	vi
IV.	Definitions, abbreviations and acronyms.....	vi
A.	Policy management powers.....	1
B.	Scope and objectives	1
C.	Data controller.....	1
D.	Data protection officer.....	1
E.	Personal data collected and processed.....	2
F.	Means of data collection	2
G.	Purposes of data processing	3
G.1.	Processing for contract performance purposes.....	3
G.2.	Processing based on a legal obligation.....	4
G.3.	Processing based on the legitimate interest of the Bank.....	4
H.	Consent of the data subject	5
I.	Cookies Policy	6
I.1.	Definition of cookies	6
I.2.	Management of cookies	6
I.3.	Types of cookies used on the Bank’s website	6
I.4.	Management of cookies	7
J.	Transmission of personal data by the Bank.....	7
K.	Personal data protection measures	8
L.	Limits for the storage and processing of personal data.....	8
M.	Rights of data subjects	9

< This page intentionally left blank >

Privacy Policy

Board of Directors

I. Versions Index

Date	Version	Description
Out.2022	1	Creation of document based on the information disclosed to the public in the form of questions and answers on the Bank's website

II. Properties

Proprietorship

Board of Directors

Proponent

Governance and Information Security Committee

Contributors

Data Protection Officer

Approval

Board of Directors, on 31 October 2022

Banco Carregosa Code

Policy Rules | 2.15

Entry into effect

1 November 2022

Scope of Disclosure

Public

III. Legislative sources and reference documents

1.07 – Organisation and Internal Governance.

1.12 – Outsourcing Policy.

1.19 – Business Continuity Plan.

1.4 – Operational Risk Management Policy.

1.41 – Information Governance Policy.

2.11 – Employee Data Protection Policy.

2.01 – Code of Conduct.

2.09 – Policy on the Reporting of Irregularities.

2.12 - Information Security Policy.

Banco de Portugal Notice No. 3/2020, of 15 July 2020, regulating the internal governance and control systems and defining the minimum standards on which the organisational culture of entities subject to Banco de Portugal's supervision must be based.

Directive 2014/65/EU of the European Parliament and the Council of 15 May 2014 on markets in financial instruments – DMIF II.

Law No 34/2013, of 16 May, establishing the regime for the exercise of private security activity.

Law No 58/2019, of 8 August, which ensures the implementation, in the national legal system, of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016.

EBA guidelines on internal governance (EBA/GL/2021/05), published in Circular Letter CC/2021/0000057.

Legal Framework of Credit Institutions and Financial Companies, approved by Decree-Law No 298/92, of 31 December.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data – GDPR.

IV. Definitions, abbreviations, and acronyms

Bank or **Banco Carregosa**: Banco L. J. Carregosa, S.A.

BdP: Banco de Portugal.

BoD: Board of Directors.

CMVM: Portuguese Securities Market Commission.

Employees: any person with employment ties to the Bank, irrespective of the hierarchical function or nature and duration of this tie, including, pursuant to applicable legal, regulatory or contractual provisions, agents, commissioners and permanent or one-off service providers under an outsourcing arrangement.

Policy: this Privacy Policy.

RGICSF: Legal Framework of Credit Institutions and Financial Companies.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

SMS: Short Message Service.

A. Policy management powers

1. The BoD is responsible for approving this Policy.
2. The BoD shall also be responsible for ensuring:
 - i. The periodic review of this Policy, at least every two years, without prejudice to reviews justified by legal or regulatory changes;
 - ii. The dissemination of this Policy to all the employees, as well as on the Bank's web page;
3. The internal disclosure of the Privacy Policy shall be carried out by making it available in the Bank's document management tool.
4. Banco Carregosa reserves the right to amend this document at any time to bring it into line with best market practices or legislative or regulatory changes. Where changes are relevant and substantive, the Bank shall make reasonable and appropriate efforts to inform the data subjects using the normal channels and mechanisms for contacts between the Bank and its clients.

B. Scope and objectives

5. This Policy reflects the Bank's commitment to:
 - i. Inform, in a transparent manner, about the personal data it collects and processes and under what conditions;
 - ii. Ensure the security of personal data and the privacy of data subjects;
 - iii. Provide appropriate mechanisms for the exercise of the rights of the data subjects;
 - iv. Respect the provisions of the GDPR and other applicable legislation, including the national legislation that complements it – Law No 58/2019 of 8 August;
 - v. Comply with the duties of confidentiality arising from the Legal framework of Credit Institutions and Financial Companies approved by Decree-Law No 298/92 of 31 December 1992.

C. Data Controller

6. Banco Carregosa is responsible for processing the personal data of its employees, prospective employees, clients, potential clients and/or former clients. The Bank's contact details are as follows:

Address: Avenida da Boavista,

1083 4100-129, Porto

Telephone: 22 608 6460

Email: info@bancocarregosa.com

D. Data Protection Officer

7. Banco Carregosa has appointed a Data Protection Officer, who is in charge of monitoring compliance with the legislation, managing the interaction of data collected from data subjects, and for cooperating with the Portuguese Data Protection Authority, the national supervisory authority.

8. Any questions regarding the processing of personal data should be sent to the following email address: dataprotection@bancocarregosa.com.

E. Personal data collected and processed

9. Personal data is any information that, regardless of its nature or medium, directly or in combination with other data, that can identify or be associated with a natural person.
10. Table 1 | Categories of Personal Data Processed by the Bank, presents the main categories of personal data processed by the Bank in the course of its activities.

Table 1 | Categories of Personal Data Processed by the Bank

Category of Personal Data	Examples
Identification and contacts	Name, identity document number, tax identification number, photograph, signature, address, telephone contact or email address.
Biographical data	Date of birth, nationality, place of birth, marital status, gender, household information, academic qualifications, curriculum vitae, or employment data.
Financial data	Financial wealth, responsibilities in the financial sector, or monthly salary.
Products and services	Account number, credit card number and other information regarding products and services purchased or subscribed by the client (e.g. duration and interest rate of a loan).
Transactions	Date, time, description and value of bank transactions (e.g. deposits, withdrawals, transfers, payments).
Segments and profiles	Business segment, profile or degree of credit risk, investor profile, or propensity to purchase financial products.
Opinions and preferences	Comments on the Bank's social media, or responses to satisfaction questionnaires.
Contents	Information contained in written communications between the client and the Bank, recorded calls (video and/or audio) telephone (e.g. orders relating to financial instruments transmitted by telephone).
Images	Images collected via vide-surveillance cameras placed in our premises.
Access credentials	User account, user authentication credentials.
Use of websites and applications	Pages visited, or information about the equipment used (e.g. IP address, date and duration of the visit; geographical location, browser used).
Biometric data	Collected for physical or logical access controls (e.g. face recognition).

F. Means of data collection

11. The Bank collects personal data through the means shown in Table 2 | Means of Data Collection.

Table 2 | Means of Data Collection

Means of Collection	Examples
Data provided directly by the data subjects	<ul style="list-style-type: none"> i. In completing the online and in-person account opening forms; ii. In the process of subscribing to or acquiring products and services; iii. In the interactions with client managers and visits to our premises; iv. In the letters or emails sent; v. When participating in the Bank's promotional activities, including competitions;

Means of Collection	Examples
	<ul style="list-style-type: none"> vi. In responses to satisfaction surveys; vii. In the submission of proposals to provide services to the Bank; viii. In the submission of job applications with the Bank.
Data collected when data subjects use products and services	Data on banking operations and transactions carried out by data subjects with the Bank (e.g. deposits, withdrawals, transfers, payments, credit contracts, provision of guarantees).
Profiling	Data produced by the Bank through the application of analytical models to data subjects' data and data relating to the use of the Bank's products and services by data subjects.
Cookies	Data relating to the use of the Bank's website and applications e.g. pages visited; user preferences), obtained via the Bank's cookies or those of third parties. More information on the type of cookies used by the Bank and on the data collected can be found in Section I – Cookies Policy.
Data obtained from third parties	Data obtained by the Bank from third parties with whom th Bank works, including Banco de Portugal, public authorities, agents working on behalf of the Bank, or Bank partners in connection with events or competitions.

G. Purposes of data processing

12. Pursuant to the GDPR, processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
13. Promotes the lawful and transparent processing of your data, using validated forms of legitimation and using them only for the purpose described in this Section.

G.1. Processing for contract performance purposes

14. Some personal data are processed by the Bank as they are necessary for the conclusion, performance and management of contracts to which the data subject is a party or for carrying out pre-contractual proceedings at the request of the data subject, such as:
 - i. Opening of accounts and recording and preservation of information necessary for the provision of banking and financial intermediation services;
 - ii. Provision of information as part of the marketing of products and services provided by the Bank, and investigation as to whether that are suitable to the client's profile;
 - iii. Management of the business relation through the recording of banking operations, in particular: transfers, transfer of titles, cheque and cash deposits, execution of orders in financial instruments;
 - iv. Analysis and response to complaints, requests for clarification and suggestions;
 - v. Adherence to services linked to electronic channels, such as homebanking and e-trading platforms;
 - vi. Management of credit operations, in particular as regards the simulation, contracting, recovery and the provision of associated guarantees.

G.2. Processing based on a legal obligation

15. Banco Carregosa's activity is subject to a set of legal requirements under which the Bank has to collect and process a set of data, namely:
 - i. Legislation on the prevention of money laundering and terrorist financing;
 - ii. The body of legislation on financial intermediation, headed by the Second Markets in Financial Instruments Directive (DMIF II);
 - iii. Tax legislation;
 - iv. Legislation applicable to the exercise of the banking activity, especially the Legal Framework of Credit Institutions and Financial Companies;
 - v. Requirements concerning the compulsory adoption of security measures at the facilities;
 - vi. Provisions relating to the supervision of banking activity and other regulatory obligations to which it is also subject, issued namely by Banco de Portugal, the European Central Bank, the European Banking Authority, the Portuguese Securities Market Commission, the European Market Supervisory Authority and the Competition Authority;
16. Examples of processing based on legal obligations:
 - i. Determining risk profiles and ascertaining knowledge, experience and investment objectives for the acquisition of certain financial instruments;
 - ii. Using screening and filtering tools to prevent crimes related to money laundering and terrorist financing;
 - iii. Detection, analysis and response to potential fraud events, in particular those related to remote operations (e.g. credit card transactions, or homebanking);
 - iv. Provision of information and responding to requests from public authorities – Provision of mandatory information (prudential and other) and in response to various requests from sector regulators (e.g. Bank of Portugal, European Central Bank, CMVM), public authorities (e.g. Courts, Police, tax authority), external auditors, or under The Foreign Account Tax Compliance Act, 2020 (FATCA) or the Common Reporting Standard (CRS);
 - v. Compliance with tax and accounting obligations;
 - vi. Video surveillance of the Bank's physical premises, with a view to protecting people and property and preventing crimes, allowing evidence to be gathered. As established in Law No 34/2013, the cameras installed ensure the identification of people and coverage of public attendance areas, deposit and safekeeping of valuables and vaults, cash dispensers and control of access and permanence in the respective areas;
 - vii. Registering and recording of communications carried out when placing orders in financial instruments;
 - viii. Collection, classification and storage of physical documents containing personal data in the documentary archive, which constitute mandatory evidence in the context of the Bank's activity.

G.3. Processing based on the legitimate interest of the Bank

17. Data processing carried out based on the legitimate interest of the Bank is primarily aimed at continuously improving the business relationship and client experience, unless the interests or fundamental rights and freedoms of the data subject prevail and require the protection of personal data, requiring personal data protection prevail in particular if the data subject is a minor.

18. Examples of processing in the Bank's legitimate interest:
- i. Providing information to clients on financial markets, technical analyses, products and services;
 - ii. Sending marketing communications via SMS and email on promotional campaigns or aimed at boosting the purchase of the products and services offered by the Bank;
 - iii. Using the historical data of interactions with clients and the financial information collected to define profiles and categories to increase the quality of communications and services provided;
 - iv. Checking the levels of satisfaction and the quality of services provided;
 - v. Managing defaults (litigation) or the exercise/defence of a right, regardless of whether it is a legal proceeding or an administrative out-of-court proceeding;
 - vi. Accessing credit information systems in determining credit risk;
 - vii. Keeping and managing information systems to protect their integrity, namely through access control and monitoring;
 - viii. Managing and monitoring of information systems and technological infrastructures, recording of events of access and use of the systems, detection, analysis and response processes to potential information security incidents, control of identities and access to the bank's information systems, or control of physical access to facilities;
 - ix. Other legal grounds for processing personal data set out in the GDPR:
 - a. Where processing of data is necessary to protect a vital interest of the data subject or of any other person;
 - b. Where processing is carried out in the public interest and is done by a compliance officer vested with public authority.

H. Consent of the Data Subject

19. The data subject may allow the Bank to process certain data by giving their free, express, informed, specific – oral – consent or by other verifiable means:
20. Examples of processing based on the data subject's consent:
- i. Collection of biometric data for the purpose of authenticating access to homebanking and validating operations;
 - ii. Adapting the browsing experience on the Bank's website, according to:
 - a. The counting of number of visits to the website, visitor origin, site viewing time and the pages consulted within the website;
 - b. The optimisation of contents, based on the browsing history; and
 - c. The optimisation of browsing based on the operative systems and browsers used.
 - iii. Call recording as a means of proof of information or instructions transmitted in the context of a pre-contractual relationship (e.g. proof of identity of the data subject), instructions transmitted in the context of a contractual relationship (e.g. orders on financial instruments) or with a view to monitoring the quality of services.

21. If the data subject is a client of the Bank, they can withdraw consent for the processing of data collected based on this form of legitimation through their homebanking, under the "Setting" tab, or by contacting the Data Controller.
22. If the data subject does not have access to the homebanking service, they can manage the topics of interest they have subscribed and consented to using the link provided in the Bank's marketing communications.
23. For the above situations or others not listed above, the data subject must contact the Data Protection Officer.

I. Cookies Policy

I.1. Definition of cookies

24. Cookies are small text files that are placed by websites visited on users' computers or mobile devices through the internet browser. They allow the website to recognise the device the next time users access it to make websites work faster and more efficiently without the need to repeatedly enter the same information.

I.2. Management of cookies

25. Users may, at any time and through their browser choose to be notified about cookies received, as well as block them in whole or in part from entering their system (even if they have authorised it before). To do this, please see the browser Settings/Tools, in the Privacy section. Please note, however, that refusal to use cookies on the website may result in the inability to access some of its areas or receive customised information.

I.3. Types of cookies used on the Bank's website

26. **Strictly necessary cookies** — These cookies are necessary for the website to work and cannot be turned off on our systems. They are usually only set in response to actions taken by the user and which correspond to a request for services, such as setting their privacy preferences, logging in or filling in forms. Users can set their browser to block or alert them to these cookies, but some parts of the website will not work if they do. These cookies do not store any personally identifiable information.
27. **Performance cookies** — These cookies allow the Bank to count visits and identify traffic sources so that the website's performance can be measured and improved. Their use helps the Bank know which pages are the most and least popular and see how visitors move around the website. All information collected by these cookies are aggregate and, therefore, anonymous. The cookies used do not collect information that identifies the user and only contain generic information, such as how users enter and use the website or in which part of the country and/or countries they access the site. In effect, the information obtained only relates to the user's preferences.
28. **Functionality cookies** — These cookies enable the website to provide enhanced functionality and personalisation. They may be set by the Bank or by third-party providers whose services the Bank has added to its pages. If users do not allow these cookies, some or even all of these features may not work properly.
29. **Targeting cookies** — These cookies may be set in the Bank's website by its advertising partners. They may be used by those companies to build a profile of users' interests and show relevant adverts

on other websites. These cookies do not directly store personal information, but are based on uniquely identifying the device used. If users do not allow these cookies, they will receive less targeted advertising.

30. **Social Media cookies** — These cookies are set by a range of social media services added to the website to allow the sharing of contents. They are capable of tracking users' browsers across other sites and building a profile of their interests. This may impact the experience and contents views on other websites. If users do not allow these cookies, the use of sharing tools may be inhibited.

I.4. Management of cookies

31. Users may, at any time and through their browser, choose to be notified about cookies received, as well as block the use thereof in whole or in part through the Settings/Tools on the browser, in the Privacy section. Refusal to use cookies on the website may result in the inability to access some of its areas or receive customised information.
32. All browsers allow users to accept, refuse or delete cookies, notably by selecting the appropriate settings. Cookies can be configured in the browser in the "Options" or "Preferences" menu. Note, however, that disabling cookies may prevent some services on the Bank's website from working properly, affecting navigation in part or in full.
33. Updated instructions on how to manage cookies in the most commonly used browsers are available on the Bank's website.

J. Transmission of personal data by the Bank

34. The Bank allows access to personal data to employees who need them to perform their duties, namely in the context of contractual, pre-contractual and legal activities or obligations of the Bank. Additionally, personal data may be transmitted to third parties, namely:
- i. To companies controlled or held by the Bank, within the scope of measures to prevent money laundering, terrorist financing and fraud, or for administrative and financial management purposes at Group level;
 - ii. To financial entities located in a Member State of the European Union or in an equivalent third country, within the scope of measures to prevent money laundering and terrorist financing, when the information concerns a client or a common operation and provided that confidentiality is ensured under the same terms as those applicable to Banco Carregosa;
 - iii. To public authorities and supervisory institutions (e.g. Banco de Portugal, European Banking Entity, European Central Bank, Portuguese Securities Market Commission, and tax authorities), whenever there is a legal or regulatory obligation to do so, for example, for the communication of information:
 - a. To the Accounts Database, the Central Credit Register and the List of Cheque Users presenting a Risk (LUR – Portuguese acronym for "Listagem de Utilizadores de cheques que oferecem Risco"), pursuant to the applicable law;
 - b. In the course of an investigation, reporting or proceeding, to Public Bodies, the Court and the Security Forces responsible for the matter, or
 - c. To authorities or official bodies of other countries, within or outside the European Union, in connection with the fight against terrorist financing, serious organised crime and the prevention of money laundering.

- iv. To other credit and financial service institutions for the execution of the contractual relationship with the client or for the provision of complementary benefits and/or those derived from the contracted product or service, under the terms set out in the respective contracts;
 - v. To subcontractors and service providers acting on behalf of or under the instructions of the Bank (e.g. technological service providers), where necessary for the execution of financial intermediation and banking services contracts.
35. The transmission of data to countries outside the European Union may only occur where necessary:
- a. For the execution or orders or requests (e.g. transferring payments abroad);
 - b. By legal requirements, or
 - c. With the express authorisation of the data subject.
36. Where service providers from third countries must be used, Banco Carregosa will contractually ensure that these entities comply with all legal obligations on data protection. The metadata collected during the use of the Banco Carregosa website may be transmitted to third parties, namely Google, Youtube, Vimeo, Facebook, Instagram, LinkedIn, Twitter and Havas Media Group companies.
37. Where requested by data subjects, the Banco will identify the subcontractors used by the Bank in the provision of services.
38. For clarifications on the transmission of personal data by the Bank, the Data Protection Officer should be contacted.

K. Personal data protection measures

39. The protection of data confidentiality and integrity is one of the fundamental pillars in building relationships of trust with the Bank's stakeholders.
40. The Bank has in place appropriate organisational measures, processes and security systems to protect personal data against destruction, alteration and unauthorised access, including:
- i. Mechanisms for controlling access to information systems and data, based on a criterion of need and respective control of consultations;
 - ii. Special security systems (e.g. firewalls, antivirus, intrusion detection systems);
 - iii. Mechanisms to register the activities carried out by employees, clients and other users of the information system (e.g. access, amendment, deletion of personal data).

L. Limits for the storage and processing of personal data

41. The Bank retains and processes personal data for as long as necessary and as long as the legitimate purposes for which the data are processed subsist, in order to comply with contractual, legal and regulatory obligations, or to protect the legitimate interests of the Bank or third parties.
42. In the case of processing based on consent, the data will be deleted as soon as the data subject withdraws consent or exercises the right to deletion.
43. As regards the data collected based on legal requirements, the Bank complies with the greater of the legal limitation periods associated with legal, fiscal or regulatory obligations, or the periods provided for in special legislation, for example, seven years after the end of the contractual relationship provided for in the law on the prevention of money laundering and terrorist financing.

44. Additionally, pursuant to Article 6(f) of the GDPR, data relating to the use of accounts held with the Bank — including, but not limited to, bank and financial statements, proof of transactions and invoices — may be kept until the limitation period for contractual liability, which, under civil law, is set at 20 years.

M. Rights of data subjects

45. Banco Carregosa guarantees the exercise of the rights of data subjects in relation to the processing thereof — Table 3 | Rights of the Data Subjects.

Table 3 | Rights of Data Subjects

Data Subject's Rights	Description
Access	Without prejudice to the protection of the rights of third parties, Data Subjects shall have the right to access personal data that concern them, and to obtain information on the conditions of the processing thereof.
Rectification	Data Subjects have the right to request the rectification of their personal data that may be inaccurate or incomplete (e.g. address, email address, telephone contacts).
Deletion	Data Subjects have the right to the deletion of their personal data collected by Banco Carregosa, provided that there are no legal grounds for keeping them (e.g. compliance with a legal obligation, defence of the Bank or of third parties in a court case).
Limitation of processing	Clients have the right to request the limitation of data processing when (i) they have contested the accuracy of the personal data and for a period that allows Banco Carregosa to check their accuracy; (ii) the processing is unlawful and they have objected to the erasure of the personal data; (iii) the processing has already ceased, but Banco Carregosa requires the data for the purposes of stating, exercising or defending a right in a court case.
Portability	Clients have the right to receive personal data they have provided to the Bank, in a structured, commonly used and machine-readable format, and the right to transmit such data to another controller.
Objection	Data Subjects have the right to object to data processing where such processing is carried out in the public interest or in the interest of the Controller and there are no compelling legitimate grounds overriding the interests, rights and freedoms of the data subject, or the data are not necessary for the stating, exercise or defence of a right in a legal proceeding.
Withdrawal of consent	Clients have the right to withdraw the consent they have given for processing based thereon.

46. Whenever the data subject exercises any of the above rights, the Bank or the Data Protection Officer shall reply to the Data Subject within one month. In cases where the request is particularly complex, this time limit shall be extended by a further month and the reply shall be accompanied by a statement of reasons.
47. Where the Bank considers that it is not possible to comply with requests, the Data Subject shall be informed of the Bank's reasons within the time limits set out above.
48. The exercise of rights is free of charge, except where situations considered excessive, anomalous and/or in bad faith occur, in which case the Bank shall inform the Data Subject in advance of the fees to be charged and the justification thereof.

49. The Bank has appropriate mechanisms in place to check and confirm the identity of data subjects who wish to exercise their rights, and only those whose identity can be confirmed shall be attended to, and through a channel that allows proof of the request and of the respective reply.
50. If the reply of the Bank or of the Data Protection Officer is not according to the expectations of the Data Subject or if the processing operations carried out give rise to concerns, the Data Subject must lodge a complaint with the Portuguese Data Protection Authority, the competent national supervisory authority, via the following contacts:

Comissão Nacional de Proteção de Dados

Address: Av. D. Carlos I, 134 - 1.º 1200-651 Lisbon

Telephone: 213928400

Email: geral@cnpd.pt

