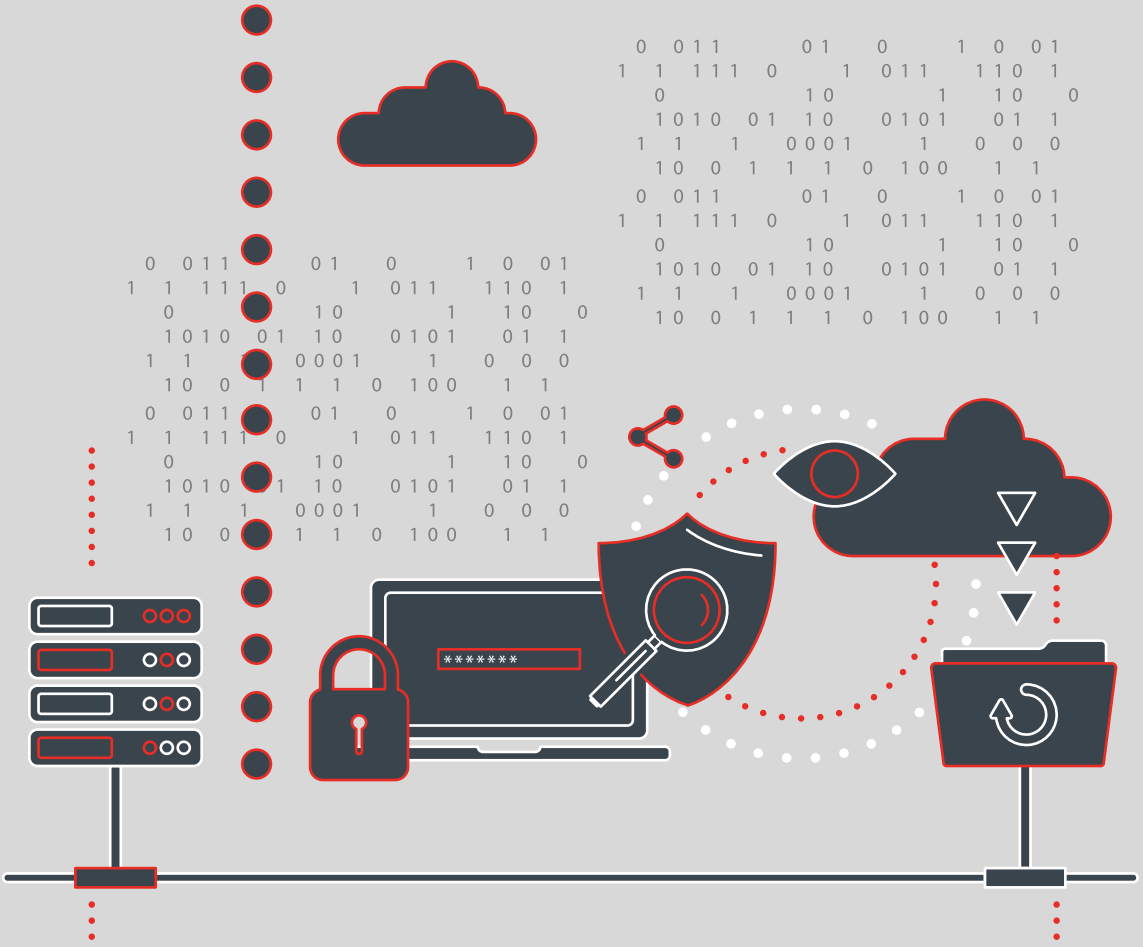
Data Protection
General Regulation



PHOENIX GROUP BRAZIL

Table of Contents

1. OBJECTIVE 2
2. FIELD OF APPLICATION 2
3. CONCEPTS AND DEFINITIONS 3
4. EXECUTION PROCEDURE 5
5. GENERAL RULES 5
6. SPECIFIC RULES ON COMPUTATION AND COMMUNICATION RESOURCES 6
7. OBLIGATIONS ON THE USE OF COMPUTATION AND COMMUNICATION RESOURCES 7
8. LIMITATIONS ON THE USES OF COMPUTATION AND COMMUNICATION RESOURCES 9
9. GENERAL RULES ON THE PROCESSING OF DATA 9
10. SPECIFIC RULES ON THE PROCESSING OF PERSONAL DATA 10
11. SPECIFIC RULES ON CONFIDENTIAL INFORMATION 12
12. PROCEDURE IN CASE OF DATA BREACH 13
13. VALIDITY 14

1. OBJECTIVE

1.1. This Policy of the Computer Use and Data Protection ("Policy") of **PHOENIX Group** reflects the rules, principles and values that should guide the attitudes, behaviors and decision making of all Employees and third parties of the **PHOENIX Group**, making our actions an example of good practices and respect for the protection of personal data and other confidential information.

1.2. In this sense, the Policy aims to incorporate into **PHOENIX Group's** internal practices, the protection of privacy, industrial secrets and privacy, as well as the awareness raising and ongoing updating of its Employees and Third Parties, in accordance with applicable Brazilian legislation, including but not limited to, the General Personal Data Protection Regulation, the Civil Code, the Consumer Protection Code and the Brazilian Civil Rights Framework for the Internet, as the case may be, in addition to the best practices adopted in international standards, such as the General Data Protection Regulation (GDPR) in force in the European Union. Therefore, this Policy should be read and interpreted in conjunction with **PHOENIX Group's** Code of Ethics and Conduct and should be used as a consultation mechanism in case of doubt regarding internal general and commercial conducts and contacts with **PHOENIX Group's** Clients, competitors, Third Parties and Government Authorities.

1.3. This Policy aims to describe rules of good practice and governance setting out the conditions for organizing, operating regulations, proceedings, including data subjects' complaints and petitions, safety regulations, technical standards, specific obligations for all involved in the Treatment, education actions, internal mechanisms of supervision and risk mitigation and others aspects related to data processing.

2. FIELD OF APPLICATION

2.1. This Policy applies to Phoenix Tower Participações S.A., as well as to its subsidiaries, affiliates, associated, investees, which already exist and/or may exist or belong to Phoenix.

2.2. The Policy covers all Employees and Third-Parties, constituting an individual and collective commitment to all of these, in a manner that each one of them complies with, promoting its full compliance in all **PHOENIX Group's** actions and in its relationships with all stakeholders.

2.3. The Employees of the **PHOENIX Group** will take formal notice of this Policy, which will be widely disseminated through print and electronic means. Failure to comply with the rules, principles and commitments set forth in this Policy may result in the adoption of disciplinary measures, in accordance with **PHOENIX Group's** standards. The **Group** will periodically review this Policy with transparency and stakeholder participation.

3. CONCEPTS AND DEFINITIONS

For the purposes of this Policy, the terms listed below have the following meanings, and may be used regardless of gender or quantity, as the case may be:

- **National Authority of Data Protection:** public administration organ responsible to protect, implement and supervise the compliance of the General Personal Data Protection Regulation.
- **Government Authority**[1]: every organ, Department or entity of the direct, indirect or foundational administration of any of the powers of the Union, States, Federal District, municipalities, Territories, legal entity incorporated into public assets or entity to whose creation either costs or the treasury has competed or competes with more than 50% (fifty percent) of the equity or annual income; as well as the organs, State entities or the diplomatic representations of a foreign country, as well as organs, entities and legal entities controlled, directly or indirectly, by the Government of a foreign country or international public organizations, including sovereign wealth funds or an entity whose property is a sovereign fund.
- **Employee**: all members of the Boards of Directors, the Audit Committee, the Executive Boards, as well as the occupants of managerial functions, employees and trainees of the **PHOENIX Group**.
- **Data:** Any type of data or information, including Personal Data, Anonymized Data, Sensitive Data and Confidential Information.
- **Anonymized Data**: Personal Data relating to a holder that cannot be identified, considering the use of reasonable technical means and available at the time of its treatment.
- **Personal Data**: information related to the natural person identified or identifiable, including Employees and Third Parties that work with **PHOENIX Group**.
- **Sensitive Personal Data**: Personal data on racial or ethnic origin, religious beliefs, political opinions, membership of trade unions or organizations of a religious, philosophical or political nature, data on health or sex life, genetic or biometric data, when linked to a natural person.
- **Party responsible for Data**: role played by *General Counsel* Vice-President, following the guidelines of the **PHOENIX Group's** Board of Directors, for acts as a communications channel between the companies of the **Group**, the Personal Data Holders and the National Authorities of Data Protection and to adopt the necessary measures and to guide all employees of the **PHOENIX Group's** about the practices to be taken in relation the data protection.
- **Responsible Technician**: natural person, indicated by the **PHOENIX Group**, which, acting in conjunction with the information technology area and following the guidelines of the senior management of the **PHOENIX Group** and the person

[1] Examples: Ministries, Secretariat, Regulatory Agencies, Companies such as SABESP, CEDAE, SANASA, Banco do Brasil, BNDES, Authorized, Concessionaires or Permissionaires of Public Services, international organizations such as the World Bank, IMF, United Nations, among others

in charge of data, is responsible for the supervision of compliance with the determinations present here, by monitoring of data, by the evaluation of internal and external vulnerability, the development of plans of response to data breach, for supporting the person in charge of data in training and awareness raising of employees and third parties, for supervising the entire technical process of Data, among others that are recommended for the protection of the environment and of the confidentiality of the data, and by assisting the person in charge with the technical aspects of all its functions.

- **Confidential information**: information and documents of legal or natural persons obtained by the companies of the **PHOENIX Group** through a contractual relationship, including those that may be used in commerce or industry, such as contracts, business plans, databases, or physical and electronic communications, other than public information, or which are not considered confidential under the terms of the agreement between the parties. In addition, **PHOENIX Group's** information and documents that, by their nature, are not intended for general disclosure or that are clearly marked as confidential, such as contracts, business plans and accounting information.
- **Data Operator**: the natural or legal person who performs the Personal Data Processing on behalf of the **Group**.
- **Computer and Communication Resources**: computers, communication systems (including landline and cell phone, *email*, video conferencing, instant messaging and internet access, including remote access) and technology (including *hardware*, *software* and other information systems) that are owned or otherwise provided by **PHOENIX Group** for the use of its Employees and, possibly, Third Parties that work with the **Group**.
- **Information Technology**: The **PHOENIX Group's** Employees team responsible for managing Computer and Communication Resources.
- **Third party**: any individual or legal entity that is not a member of the staff as an Employee or is not a member of the **PHOENIX Group** but who is contracted to assist in the performance of **PHOENIX Group's** activities, such as partners, representatives, suppliers, consultants, service providers in general, sub-contracted parties, civil society organizations (NGOs), among others.
- **Data Subject**: natural person, identified or identifiable, to who concerning the Personal Data.
- **Processing**: any operation performed with Personal Data or confidential information, such as that relating to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, modification, communication, transfer, dissemination or extraction.
- **Data Breach**: any incident, irrespective of the nature or cause, that leads to or permits the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data or confidential information transmitted, stored or otherwise treated.

4. EXECUTION PROCEDURE

4.1. Violation of any determinations described in this Policy may result in disciplinary actions described in **PHOENIX Group's** other standards and policies, as well as sanctions in the terms of current legislation. For the application of any disciplinary actions and/or sanctions, the **Group** will take into account the seriousness of the breach, damage and/or injury actually caused, and the degree of guilt or bad faith of the responsible Employee.

4.2. The bodies responsible for processing complaints of transgressions will preserve the anonymity of the complainant in order to avoid retaliation against the complainant and inform him of the measures taken.

4.3. It is the employee's right to have his/her identity preserved when making any complaint and/or making denouncements anonymously. However, if the report is made anonymously, it must provide as many details as possible, including a copy of all documents that may be pertinent to the matter.

4.4. Any type of retaliation, threats or revenge is strictly prohibited against any Employee who, in good faith, is or has in any way assisted in the process of ascertaining a possible violation of this Policy.

4.5. Complaints should be forwarded to the Person in charge of Data and Responsible Technician through the Digital Data Protection Channel - protecaodedados@phoenixtower.com.br, or by means of a letter addressed directly to the Person in charge of Data.

4.6. When a report involves any facts that threaten the integrity, security and / or confidentiality of the Data or any Computation and Communication Resource, including but not limited to cases of suspected unauthorized access to any Computation and Communication Resource, the denouncing Contributor shall, in addition to submitting the complaint in the manner described in item 4.5 above, also immediately communicate what has happened to the area of Information Technology and the Responsible Technician. This includes, for example, if there is suspicion of unauthorized access to any Computation and Communication Resource.

5. GENERAL RULES

5.1. This Policy must be read, acknowledged and received by all Employees, at the time of their employment, and by any Third Parties, prior to the provision of any service.

5.1.1. The professional responsible for ensuring this reading shall, in all such situations, receive and file in an organized manner, a receipt that guarantees that the Employee or Third Party is aware of all the terms of this Policy.

5.2. Any agreements with Third Parties that involved Personal Data Processing or

Confidential Information shall contain a specific contractual clause in which the Third Party undertakes to acknowledge and comply with this Policy and assumes the responsibility of any subcontractor to do so.

5.3. All contracts with **PHOENIX Group's** customers must contain, within the business limits imposed on each case, a clause in which the customer agrees to the use of his Data, including any Personal Data, for **PHOENIX Group's** internal purposes such as management, contact and organization, and exempts the **Group** from any liability in case of any incidents involving Personal Data because of acts caused by fault of the customers.

5.4. An updated version of this Policy will be on the **PHOENIX Group's** intranet and any substantial changes thereto will be communicated by any means available.

6. SPECIFIC RULES ON COMPUTATION AND COMMUNICATION RESOURCES

6.1. The Computation and Communication Resources are intended for strictly professional purposes and linked to the activities of its Employees and Third Parties that may use them. Any Employee or Third Party using the Computation and Communication Resources declares that it understands the professional nature of these features and will use them only to fulfill their functions and obligations to **PHOENIX Group**.

6.2. Messages, Data, files and other materials that are present or were present in the Computation and Communication Resources are owned by **PHOENIX Group**, regardless of whether the user intended to make personal use of these resources. This includes material created, transmitted, or received by Internet-based systems that are accessed through Computation and Communication Resources.

6.2.1. If the user does not wish any material to be accessed by **PHOENIX Group**, Computation and Communication Resources should not be used to create, transmit, receive or store such material.

6.2.2. The use of Computation and Communication Resources is periodically and intermittently monitored for unusual activity or by means or uses that violate this Policy or any other **PHOENIX Group's** standards. Considering this, users should know that any of their communications that are made through the Computation and Communication Resources may be viewed by other Employees, regardless of their nature.

6.3. The **PHOENIX Group** has the right to browse, open, review, monitor, save, record, use or make available any document, voice message, *email*, text message or file of any format that has been created, stored, transmitted or received by its Employees or by Third Parties while using the Computation and Communication Resources.

6.3.1. The Users understand and admit as far as they include their Personal Data in

Computing and Communication Resources, such data may used by **PHOENIX Group**, including other Employees or Third Parties, as appropriate.

6.4. Any Third Party that needs to use the Computation and Communication Resources should have only the necessary access to them so that they can carry out their activities. Data access to Third Parties shall be granted only for the period strictly necessary and as long as such Third Party maintains a valid and effective contractual and/or commercial relationship with **PHOENIX Group**.

6.5. The use of the Computation and Communication Resources in disagreement with this Policy may lead to disciplinary sanctions under the Execution Procedure set forth in this Policy as well as other **PHOENIX Group's** policies in force and may result in termination of employment and/or provision of service contracts, as appropriate, in accordance with the legislation and with the contractual determinations, as already expressed in clause 4.1 of this Policy.

6.6. Any Employees or Third Parties who for any reason no longer work for **PHOENIX Group** or are absent from work will not be able to access Computing and Communication Resources, shall the Information Technology area suspend, immediately, the access to such Employees or Third Parties.

7. OBLIGATIONS ON THE USE OF COMPUTATION AND COMMUNICATION RESOURCES

7.1. The use of Computation and Communication Resources should always be done according to the orientation of the Information Technology area, including, but not limited to, the installation of *software* - which must be carried out only with the authorization of the area of Information Technology, equipment care, remote access and configuration of *email* on mobile devices.

7.2. The Employees are responsible for preserving any Confidential Information maintained in the Computation and Communication Resources, following the obligations contained in this Policy. If there is doubt whether a document or information consists of Confidential Information, it should be treated as if it were. Whenever possible, Employees should indicate in the name of a document, its confidentiality or protect documents by password. The improper attempt to access a password-protected document is strictly prohibited and may lead to the application of applicable legal and contractual sanctions under the terms of the Enforcement Procedure set forth in this Policy and other **PHOENIX Group's** policies and standards.

7.3. Employees and/or Third Parties, where applicable, must take special care to ensure that applications or tools in which they perform *uploads* "to the cloud" or to other devices are not used in a manner to create vulnerabilities for Confidential Information, including, but not limited to, file format conversion sites. If there is any concern about the possibility of documents or the like in Computation and Communication Resources being leaked, the Employee and/or the Third Party shall immediately communicate to the Information

Technology department and its manager.

7.4. In the event that the Contributor is removed from or disconnected from **PHOENIX Group** for any reason, or in the event of a contract with Third Parties terminating, no Computation and Communication Resource may be accessed and/or taken so that any document or information that has been accessed and/or withdrawn shall be returned to **PHOENIX Group** and deleted in the presence of an authorized Phoenix representative.

7.5. Employees and Third Parties using the Computation and Communication Resources shall ensure the security of the resources and information present on **PHOENIX Group** systems, including changing their passwords periodically and performing *log off* of the systems when they are not using them.

7.5.1. Any passwords or digital certificates used to access the Computation and Communication Resources are the sole responsibility of their holders.

7.5.2. If there is any suspicion of loss of mobile devices or that someone may have undue access due to lack of care regarding these digital passwords and certificates, this must be immediately communicated to the Information Technology area.

7.6. Employees and any Third Party who may use Computation and Communication Resources shall ensure their integrity and use them with all due care and diligence, always following any instructions of the area of Information Technology.

7.7. In order to perform communications and other tasks related to their duties at **PHOENIX Group**, Employees shall use only the Computation and Communication Resources, including corporate *email* accounts, the use of personal tools for communication on behalf of the **Group** with Third Parties, including but not limited to communications applications not approved by the Information Technology area, is prohibited. The use of any tools not included in the Computation and Communication Resources for the sharing of Data is expressly prohibited, including but not limited to sending photos of documents or proposals between Employees and Third Parties.

7.8. The Information Technology area will take all reasonable steps to implement this Policy and maintain the security of Computation and Communication Resources, including:

- Separation of *email* messages between "internal" and "external";
- Blocking USB ports from any corporate computers and notebooks;
- Implementation of *disclaimer* in the automatic signature of *email* of employees highlighting the confidential nature of the communication; and
- Blocking the installation of any executable *software* without previous authorization of the Information Technology area.

8. LIMITATIONS ON THE USES OF COMPUTATION AND COMMUNICATION RESOURCES

8.1. The following uses of Computation and Communication Resources are strictly prohibited:

a. Disclosing or publishing any **PHOENIX Group** or Third-Party Confidential Information through Computation and Communication Resources.
b. Searching, viewing or saving documents, Data (including Personal Data), voice or text messages, or *emails* that are not yours, in Computation and Communication Resources, without a legitimate objective according to your scope of work.
c. Copying, on personal devices, documents, data, voice or text messages, or *emails* accessed through Computation and Communication Resources.
d. Sending or forwarding *emails* or documents that may constitute Confidential Information for your personal *email* or using *email* for professional communications related to these types of documents.
e. Sending, forwarding or taking action to receive any message of racist, violent, discriminatory, abusive, pornographic, obscene or illegal content, or contains an offensive language or image, or has been used with the intention of intimidating any person or creating an oppressive work environment.
f. Download any program not previously approved or at odds with **PHOENIX Group** Information Technology department guidelines.
g. Copying or reproducing material protected by intellectual property right, including copyright or trademark, without authorization.
h. Presenting personal opinions, political convictions, philosophical or religious beliefs, unrelated to the activities of the Employee or Third Party in **PHOENIX Group**, in any context that makes such opinions appear to be that of the **Group**.
i. Sending or forwarding any type of *spam*, viruses, *malware*, *phishing* or any other type of code that exploits or creates vulnerabilities in Computation and Communication Resources.

9. GENERAL RULES ON THE PROCESSING OF DATA

9.1. This Policy shall be an integral part of any contract with Third Parties that involves Data and shall be initialed on each page upon signature of the agreement, which shall contain specific determination and obliging the Third Party to respect all its determinations. No contract involving Data may be entered into with Third Parties that do not commit to following this Policy.

9.2. Contracts with Third Parties shall guarantee that, at the end of the contract and termination of the relationship between the parties, Third Parties shall return or destroy all Data that they have received as a result of the contract, and, as the case may be, ensure that subcontracted parties that have received the Data with the express permission of **PHOENIX Group** do the same.

9.3. Further, contracts with Third Parties shall ensure that they will not collect or otherwise in any way process Data on behalf of **PHOENIX Group** except as expressly authorized by the **Group**.

9.4. Data Operators will may never access, view, use, or otherwise perform any Data Processing which is not absolutely necessary for any **PHOENIX Group** task, service or **PHOENIX Group**'s contract acquisition. In addition, whenever the Data Operator is a Third Party, it shall have its access to the Data collected or stored by the **Group** reduced to the minimum necessary to meet its contractual obligations to the Companies of the **PHOENIX Group**.

9.5. Employees and Third Parties who do not have, as part of their functions, those related to Data Processing shall not, under any circumstances, access, view, use, or otherwise do any Data Processing except as strictly necessary due to some maintenance or monitoring task, in which cases only access and visualization to these Data will be allowed.

9.6. Following the rules regarding Computation and Communication Resources, Data Operators shall not, under any circumstances, copy Data to devices of personal use, nor send or forward Data or *emails* containing any type of Data to anyone who has not been previously and expressly authorized by Phoenix to receive such Data. Likewise, Data Operators shall not, under any circumstances, send or forward Data or *emails* containing some type of Data to their personal *emails*, or use *emails* to send information of this nature.

10. SPECIFIC RULES ON THE PROCESSING OF PERSONAL DATA

10.1. All the companies of the **PHOENIX Group** are companies committed to preserving the intimacy, privacy and image of the human person. Accordingly, all Third Parties and Employees must take all the care provided in this Policy or dictated by the best market practices when collecting, using, viewing, treating, transferring, anonymizing or in any way performing the Processing of Personal Data. Whenever possible, in view of the purpose of the Processing, the Personal Data shall be converted into anonymized Data by Data Operators with the express authorization of the **Group**.

10.2. The **PHOENIX Group** will appoint an Employee or a Third Party as Data Administrator and one as Responsible Technician, who will have the duties set forth in this Policy.

10.3. The **PHOENIX Group** may, eventually, transfer or share Personal Data with third parties. In addition, it may also transfer or share Personal Data with companies of the **Group**. In both situations, Personal Data can be transferred both inside and outside of Brazil. All collection of Personal Data must inform the holders of Personal Data of these possibilities and the purposes for which Personal Data will be transferred.

10.3.1. Employees and Third Parties understand and agree, by signing this Policy to receive this Policy, that **PHOENIX Group** may collect, use, process, store and transfer its Personal Data to third parties within and outside the country only to

the extent that it is strictly necessary for the management of Employees and Third Parties and for the attainment of contracts with Third Parties and the employment contracts with Employees. For the purposes of this Policy, Personal Data that is not required for the management of Employees and Third Parties and for the attainment of contracts with **PHOENIX Group** will not be transferred.

10.3.2. As a consequence of this transfer, Third Parties who may have access to such information are, including, but not limited to, database managers, companies that control *software* accessed by **PHOENIX Group** in the "Software as a Service" (Saas) category, companies responsible for audits and/or Government Authorities that request or need to receive such information, according to the law.

10.4. The **PHOENIX Group** shall maintain all data allocated in a manner of secure and restricted access, in accordance with its management needs. In addition, it will maintain *back-up* of the data, and the business decisions about this *back-up- are left* to them at their sole discretion.

10.5. The **PHOENIX Group** shall also maintain an appropriate channel so that the holders of Personal Data may request information about the Processing of Personal Data, and in addition may also update information and rectify it as necessary.

10.5.1. The holders may also request cancellation or transfer of their Personal Data, and this request will be evaluated by the Data Administrator, with the assistance of the Responsible Technician, considering the applicable legislation and the technical possibility of complying with the request.

10.6. The collection of Personal Data must always be given only to the extent necessary to achieve contracts and for the preservation of business and labor relations and shall comply with the rules imposed by the management of **PHOENIX Group**. Any Personal Data that is unnecessary for the purposes of collection should be deleted or destroyed. Any Personal Data that is no longer necessary (whether for the purpose of a contract or for its obsolescence) must also be destroyed, except when there is an obligation to keep the Data for some time, in accordance with the applicable legislation.

10.7. Any collection of Personal Data, which is not limited to what is strictly necessary to comply with legal and regulatory obligations or to enable the performance of contracts or characterization of another legal base, must be preceded by obtaining consent. The **PHOENIX Group** and its Data Operators shall ensure that consent can be demonstrated at any time. All contracts or procedures that result in any collection of Personal Data, which is not limited to what is strictly necessary to comply with legal and regulatory obligations or to enable the performance of contracts or characterization of another legal base, by the **Group** shall include a clause obtaining consent for Processing of Personal Data with the objective of properly complying with the agreement.

10.8. Unless strictly necessary, for example, to perform union contribution on behalf of Employees according to applicable law, the **PHOENIX Group** will not collect any type of Sensitive Data. Any Personal Data collected that may be considered Sensitive Data shall be accessed or processed only under strict observation and guidance of the Responsible Technician.

10.9. The **PHOENIX Group** shall ensure that, in the case of countries whose legislation on the protection of Personal Data is less stringent than that present in Brazilian law and in this Policy, the person receiving the Personal Data undertakes to comply, at least, with the obligations present in this and in Brazilian legislation.

10.10. The Responsible Technician will be responsible for developing, maintaining and submitting to the Data Administrator a report describing the Data stored by **PHOENIX Group** and any Data Processing, including its purposes and bases.

10.11. Processing of Personal Data in disagreement with this Policy may lead to disciplinary sanctions under the Execution Procedure set forth in this Policy and other **PHOENIX Group** policies and may result in termination or rescission of employment or service contracts where appropriate according to the law and with the contractual provisions.

11. SPECIFIC RULES ON CONFIDENTIAL INFORMATION

11.1. Confidential Information must be treated in a manner that preserves its confidentiality as it is valuable information and may create serious problems for **PHOENIX Group**, its Employees and/or Third Parties, if used incorrectly or disclosed without authorization.

11.2. Employees and Third Parties undertake to protect the integrity and inviolability of the Confidential Information to which they have access because of their relationship with **PHOENIX Group** even after the termination of this relationship.

11.3. Without prejudice to other conduct prohibited by this Policy, any Collaborator or Third Party that provides services to **PHOENIX Group** is strictly prohibited:

a. To disclose, exploit or use Confidential Information in disagreement with this Policy, or without express permission to do so.
b. Access, in any way misleading, Third Party Confidential Information to which **PHOENIX Group** may not have access.

11.4. Employees and Third Parties that don't need, as part of their duties, access to Confidential Information shall not, under any circumstances, access, view, disclose or otherwise use the Confidential Information.

12. PROCEDURE IN CASE OF DATA BREACH

12.1. Any Data Breach or possibility of Data Breach shall be urgently and immediately communicated to the Information Technology area, and to the Responsible Technician, by means of the *email* protecaodedados@phoenixtower.com.br, which will be responsible for carrying out the initial analysis and the adoption of immediate prevention and correction measures necessary for the preservation of data and information security.

12.1.1. Considering the communication of the data breach is an essential aspect for the applicable measures being taken, if the data breach will be caused by an Employee and this one communicated immediately, according to this policy, this attitude will be considered in the application of the disciplinary measures.

12.2. Following the adoption of emergency measures for prevention and correction, the Responsible Technician Officer will prepare an incident report detailing the facts and the protective and corrective measures adopted in an emergency. This report will be given to the Data Administrator to establish the internal investigation procedure to identify potential violations of the information security rules, as well as evaluate the effectiveness of the measures adopted in an emergency and adopt the necessary measures with the internal and external organs, according to item 12.4.

12.3. Third Parties that may store or process Data on behalf of **PHOENIX Grou**p shall, in the event of Data Breach or possibility of Data Breach, promptly notify the **Group**, identifying the Data that has been or may have been compromised, and following **PHOENIX Group's** guidelines about the procedures to be taken.

12.4. In the case of Data Breach involving Personal Data, the Data Administrator should, with the assistance of the Responsible Technician, evaluate the need of notification of the violation of Personal Data to the appropriate Government Authorities, if applicable, as the case may be. In its determination to communicate or not the Data Breach to Government Authorities, the Data Administrator shall take into account the existence of applicable Authority considering the nature and origin of the Data in question and the possibility that the violation of Personal Data causes damages or risks to the rights and freedoms of individuals.

12.5. The notification referred to in clause 12.1 above shall contain:

a. The nature of the Data Breach, including, the types and amount of data breached, as well as the type and number of Personal Data owners involved, where possible determined.
b. Contact information for the Data Administrator to be contacted to provide clarification.
c. Description of possible consequences of Data Breach.
d. Description of technical and security measures adopt by the **Group** before the Data Breach for the Personal Data Protection.

e. Description of measures taken, ongoing or proposed, for **PHOENIX Group** to deal with the Data Breach, including measures to mitigate possible adverse effects.

12.6. It shall be the responsibility of the Data Administrator to keep records of any Personal Data Breaches, including their effects and the actions taken by Phoenix in relation to them. Such registration shall be available for verification by Governmental Authorities, in accordance with the law.

12.7. In the event of Data Breach involving Confidential Information, **PHOENIX Group** shall take appropriate action in the case, where appropriate and according to the orientation of the Data Administrator, to ensure the secrecy of the Confidential Information. The Data Administrator shall, with the assistance of the Responsible Technician, evaluate the appropriate measures considering the nature of the information, the breach, the applicable contractual determinations, and the technical possibilities available for the solution or mitigation of the situation.

13. VALIDITY

13.1. This Policy shall enter into force as of the date of its publication and shall remain valid until its revocation or inclusion of new determinations.