Corporate Policy - PTC	Issue Date: **8/31/2020**
Data Protection and Privacy	Identification: **PTC.013** Version - **04** Review: **3/19/2025**
Approval: Executive Committee	Classification of information: **Public**

1. PURPOSE

Establish people's privacy principles and protection of their personal data, and comply with regulatory and legal responsibilities when we process personal data.

2. APPLICATION

It applies to the entire the Grupo Carrefour Brasil and stakeholders

3. ACRONYMS AND DEFINITIONS

National Data Protection Agency (ANPD): Public administration department responsible for ensuring, implementing, and monitoring compliance with the General Data Protection Law (LGPD) in all national territory.

Controller - Natural or legal person, governed by public or private law, who is responsible for decisions regarding personal data processing.

Personal Data - All information related to the identified or identifiable natural person. In other words, the concept covers direct information, such as name, ID, CPF [Individual Taxpayer Identification Number] and address, as well as indirect information, such as location data and other electronic identifiers.

Sensitive Personal Data - Data on racial or ethnic origin, religious conviction, political opinion, trade union membership or religious organization, philosophical, or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person.

Data Protection Officer (DPO): Professional appointed by the company, responsible for the organization's data protection, acting as a communication channel between controller, data subject and ANPD.

Grupo Carrefour Brasil: Comprises the companies, headquarters, offices, distribution centers, stores and points of sale and service of Carrefour Group's businesses in Brazil (Atacadão, Carrefour Soluções Financeiras, Carrefour Varejo, E-commerce, Property and subsidiaries in general).

Holding: Subsidiary controlling the units of Grupo Carrefour Brasil.

General Data Protection Law (LGPD): Refers to Brazilian law nº 13.709, of August 14, 2018.

P&PD: Privacy and Protection of Personal Data.

PDS (Status Point): Periodic meetings to monitor projects or actions.

Privacy: Condition of what is private, personal or intimate, private life.

Privacy Program: Implementation and continuous operation of methodologies, tools and activities present in and/or related to the scope of privacy and data protection.

Impact Report to Personal Data Protection (RIPD): Report with process description of personal data processing that may create risks to civil liberties and fundamental rights, as well as measures, safeguards, and risk mitigation mechanisms.

Roadmap: Resource that highlights the organization's current position, purposes and means to achieve them, serving as a useful guide for teams to plan tasks and execute strategy.

ROPA (Records of Processing Activities): Registration of the data processing operations details for each process in business areas. Among other factors, it points out data categories, who processes them (controller/operator), how often and for what purposes, storage media, etc.

Personal data processing: Each and every operation carried out with personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or information control, modification, communication, transfer, dissemination, extraction, etc.

Personal Data Holder - Natural person to whom the personal data is subject of processing.

Operator - Natural or legal person, governed by public or private law, who processes personal data on behalf of the controller.

4. GENERAL GUIDELINES

The Group is committed in ensuring that personal data of our employees, customers, partners and shareholders are treated appropriately and securely by its Business Units and those who process personal data on their behalf, and going above and beyond to ensure that the personal data processing is supported by a robust governance structure.

In line with our Code of Ethical Conduct to further strengthen the Group's integrity culture, image construction and success of our business and in compliance with SDG 16 – Peace, Justice and Effective Institutions, we have prepared this Privacy Policy to define principles, and consequently, expected standards and behaviors regarding compliance with all applicable laws on collection, storage, use, retention, transfer and deletion (collectively referred to as "processing") of personal data in Grupo Carrefour Brasil.

In Grupo Carrefour Brasil, we routinely process personal data of our employees, suppliers, customers and other individuals with whom we work in our daily lives. Personal data typically includes any information relating to a person that allows it to be identified. This includes, for example, a subject's name, ID, CPF, telephone number or email, among others.

The General Data Protection Law (LGPD) regulates and imposes obligations to ensure that we process personal data legally and fairly, and to take extra precautions when processing particularly sensitive information about people (for example, information about health conditions). Furthermore, the Law requires us to establish an effective governance structure to ensure assertive decisions about how we use personal data.

It is important that we all know the importance of handling this information appropriately, not only to comply with privacy laws and regulations, but to be aligned with the Group's commitment to adopt good corporate governance practices and act, increasingly, in a complete and transparent way.

It is our commitment to protect the privacy rights of individuals whose data we collect and keep.

4.1 Fundamental Privacy Principles

To facilitate the recognition of good conduct and day-to-day business practices, we have created 9 essential Privacy Principles, guided by LGPD's principles, which we hope everyone complies with when processing personal data in Grupo Carrefour Brasil.

4.1.1 We should only process personal data when we have legal basis that allows us to do so.

Whenever we obtain personal data from/or about a subject, we must ensure that we have obtained it lawfully and that we have legal basis for each processing activity for which we wish to use them. We need to be aware that certain types of personal information that are particularly sensitive (such as information on health conditions or racial or ethnic origin) and may only be lawfully processed in more specific and limited cases, so we need to take extra care when handling sensitive personal data.

Legal basis:

- Consent
- Compliance with legal obligation
- Execution of public policies
- Studies by research department
- Contract execution / Pre-contractual due diligences
- Regular exercise of law
- Life protection
- Health support
- Legitimate interests of the controller/third party
- Credit protection

4.1.2. We must process data in accordance with data subjects' rights.

Data subjects have specific legal rights in relation to their personal data (for example, to access their data or to object to certain types of processing activities). We must be aware of these rights and respond effectively if a subject decides to exercise them.

4.1.3. We must inform the data subject what we will do with its personal data.

We must make sure to provide privacy notice to individuals, preferably at the point where their personal data is first collected (for example, on forms, websites, apps and security cameras), in which we explain who we are and what we intend to do with this personal information.

4.1.4. We must process personal data only for the specific purposes for which they were intended.

If we want to use personal data for any purpose other than those relating to the strictly legal obligations for which we originally collected the personal data, we will need to inform the subject and be sure that the additional purposes are not unlawful.

4.1.5. We must only collect the personal data that we need for the specified purposes only.

We should not ask for more personal data than we need (that is, we should not be excessive). If we do not need the data to achieve our intended business purpose, we must not obtain or process that data.

Ask the right questions:

- What is my purpose?
- What data is needed to achieve this purpose?
- Do I have the right to collect this data?
- Is this relevant?
- Were the holders properly informed?

4.1.6. We must ensure that all personal data we process is accurate and up to date.

We must ensure to data subjects accuracy, clarity, relevance and update, according to the need and to fulfill the processing purpose. We must be cautious when relying on information that may be incorrect because they are out of date (for example, if we have not had active engagement with a customer for a long period of time) and we must take action to update it.

4.1.7. We shall only retain personal data as long as necessary in line with the purpose(s) for which they were collected.

We must be proactive in deleting personal data that are no longer in need to process or store. For guidance on how long personal data should be kept before deletion, check your business unit's rules and procedures.

4.1.8. We must keep personal data confidential, secure and protect it against loss, destruction, accidental and malicious damage, and unauthorized disclosure.

We all have a duty to ensure that effective security is maintained. Personal data must be processed in a way that ensures appropriate security and confidentiality to prevent access to personal data by unauthorized people.

For detailed information on our security procedures and measures relating to all data, including personal data, please refer to your business unit's Information Security Policy and Sensitive Information Protection Policy.

We must not share personal data with people or organizations, including transferring personal data internationally, unless there is a legal basis for doing so and appropriate measures are in place to protect that personal data.

In addition to complying with the Social and Ethical Code for Suppliers, we must ensure that each organization we intend to share personal data with is able to properly protect the personal data transferred to it. In many cases, we expect a data sharing agreement to be implemented with appropriate data protection clauses to govern the agreements and support the due diligence to be carried out.

If the recipient is based abroad, additional controls may be required. If you have any questions, please contact the Group's Legal Department regarding appropriate contractual drafting (including data transfer agreements).

- Keep Control of Your Data:
- Deal directly with the department or person with whom the data should be shared.
- Avoid non-formal channels (for example, Whatsapp groups).

4.2. Data breach incidents

A data breach incident occurs when a security incident occurs within the organization relating to the data for which we are responsible, and which results in data breach of confidentiality, availability or integrity of one or more subjects.

If you become aware that a data breach has occurred (for example, if you believe that personal data may have been lost, disclosed, damaged or accessed without permission), you must notify the Privacy and Data Protection area immediately.

Communication channel:

4.3. Everyone’s role in data protection and privacy

All Group's employees and contractors must take time to familiarize themselves with this Policy, to read, understand and adhere to the Privacy Principles defined above.

GRUPO CARREFOUR BRASIL

Privacy risks must be considered in our day-to-day tasks and then act in accordance with applicable procedures when processing personal data.

Deviations from the company's policies may result in appropriate disciplinary measures, permitted under current legislation and in accordance with the Consequence Management Policy.

4.4. Contact for privacy concerns

Grupo Carrefour Brasil provides, through the link https://www.carrefour.com.br/central-de-privacidade, a communication channel to provide transparency on the personal data processing carried out by Group companies.

There, you'll find the Privacy Policy of each business unit. you can ask questions and make requests such as: what information we collect and process about you and the reasons and purposes for this processing.

If you don't find what you are looking for on the communication channel and would like to clarify any additional questions, please send an email to the using the Carrefour Group DPO's email address:

4.5 Personal Data Governance

Grupo Carrefour Brasil's Privacy Governance team indicates the principles that must be followed by each company in the Group, generating the Group's respective documentation and privacy rules. Also, to inform the public, especially the company's shareholders, the principles.standards and expected behaviors on compliance with all applicable laws on personal data processing in Grupo Carrefour Brasil.

The Privacy Governance program is carried out at all organizational levels and business units of Grupo Carrefour Brasil.

Clarification of questions, dissemination of good practices and other alignments between companies of Grupo Carrefour Brasil are carried out during the Status Points (PDS).

Carrefour Group's Data Protection and Privacy team must monitor the performance of Grupo Carrefour Brasil companies regarding the Privacy Program. This is done through periodic assessment of maturity level and indicators of each business unit.

The governance of Grupo Carrefour Brasil Privacy Program must be monitored through indicators. The governance metrics will aim to measure the Program's management performance, involving operational aspects and compliance aspects.

Privacy Risks management by each company of Grupo Carrefour Brasil is integrated into the Privacy Program strategy, so that it is used to define priorities to improve existing resources.

Privacy Program and Processes assessments will be carried out to ensure that each company of Grupo Carrefour Brasil has controls implemented and operating effectively. They are monitored by the Holding's P&PD team and Privacy Correspondents from each company of Grupo Carrefour Brasil, as necessary, by understanding checkpoints, participation in meetings, final report evaluations, deadlines alignment and evidence submission.

An annual training and qualification plan for DPO, Privacy and Data Protection Officer, Correspondent and support teams must be in place and structured, defining the training and courses necessary to maximize professional skills. Topics to develop and continuously update the employees include regulatory changes, good market practices, use of privacy management tools or other topics that are challenging for the team.

Members of P&PD teams must act as facilitators in promoting a culture of personal data protection in the institution, in addition to contributing to centralized decision-making, minimizing possible conflicts of interest.

Discussions will need to include the forum's understanding, with representatives from many sectors and processes of Grupo Carrefour Brasil, about the current threat scenario and what actions the company has already taken to protect data, what the current challenges are, and the actions planned for data privacy and its progress, as well as strategic recommendations.

5. RESPONSIBILITIES

Everyone has a responsibility to ensure that Grupo Carrefour Brasil respects the subject's privacy and that personal data are treated securely and in accordance with applicable laws and regulations.

The Privacy Organizational Structure adopted in Grupo Carrefour Brasil will be operationalized through a hybrid governance model, with DPO and Privacy and Data Protection Officer for the Holding, and a P&PD Correspondent for each company of Grupo Carrefour Brasil, in addition to a Privacy Forum for the Group and a Forum for each company. - Organizational structure. The hybrid model allows:

- Continuous communication and reports between Manager, Privacy and Data Protection Officer and Correspondents of each unit;
- The Manager's central view of activities/projects/workflows, while ensuring a certain degree of autonomy for Correspondents;
- Synergy between the person in charge and each business area.

Data Protection Officer (or “DPO”) of Carrefour Global Group

- Share good privacy and data protection practices for Grupo Carrefour Brasil;
- In global projects and initiatives that affect the Grupo Carrefour Brasil, interact with the local DPO and, when necessary, DPO and global CISO to make joint decisions.
- Monitor and deliberate regarding P&PD Program's assessment;
- Direct Grupo Carrefour Brasil and its business units, with their respective Privacy and Data Protection Correspondents, in compliance with this Policy and applicable legislation;
- Interact with data subjects and the National Data Protection Authority when requested;
- Report privacy and data protection incidents that may pose a relevant risk or harm to the affected data subjects to the following interested parties: ANPD, Global DPO, Global CISO and Risks Committee;
- In the event of privacy incidents, approve action plans to prevent recurrences of the same nature;
- Approve and authorize the disclosure of communications to holders involved in personal data privacy incident and/or to the public;
- Validate action plans defined by P&PD teams and business areas of each Group company that result in high or extreme residual risks;
- Sign the RIPDs and include opinion for processes that have high or extreme residual risks;
- Report extremely critical P&PD risks and the respective measures to address them to Grupo Carrefour Brasil's Risk Committee;
- Support and approve the decision to hire or appoint the Privacy and Data Protection Officer and Data Correspondent; and
- Approve the P&PD work plan/roadmap for Grupo Carrefour Brasil.

Additional Remarks

- DPO must report to the highest management level of Grupo Carrefour Brasil, working independently and with autonomy. In carrying out his/her duties, the DPO should not receive instructions on how to deal with a matter, for example, such as how the result should be obtained, how to investigate a complaint, the need to consult the supervisory authority. Furthermore, the DPO should not be instructed to adopt a certain perspective on an issue related to data protection standards;

The company must ensure that the DPO is not dismissed or penalized for carrying out his/her duties; and

- The DPO of Carrefour Brazil Group is Thiago Roberto Faria Lima, who can be contacted at email: dpo_br@carrefour.com.

6. ASSOCIATED DOCUMENTS

Grupo Carrefour Brasil Code of Ethical Conduct, available at: https://ri.grupocarrefourbrasil.com.br/governanca-corporativa/estatutos-politicas-e-codigos/

Ethics and Social Code for Our Suppliers; available at: https://conexaoeticacarrefour.com.br/files/AF2_Digital_CodigoConduta_Fornecedores_PT_v2.pdf

Risk Management Policy, Cybersecurity Policy, among other Corporate policies of Grupo Carrefour Brasil, available at: https://ri.grupocarrefourbrasil.com.br/governanca-corporativa/estatutos-politicas-e-codigos/

7. DOCUMENT REVIEW AND UPDATE

This regulation must be reviewed every three years regarding adherence to Policies, Standards, Procedures, or whenever significant changes in the processes are identified.

This Policy is a living document. Therefore, reviews, changes and adaptations may be carried out at any time, as necessary, to ensure data privacy evolution and maturity in Grupo Carrefour Brasil.

8. CONSEQUENCE RULES

Deviations from regulations may lead to appropriate disciplinary measures, permitted under current legislation and the internal rules of the Grupo Carrefour Brasil.

In cases of non-compliance with these guidelines, reports can be made at: CONEXÃO ÉTICA: Website: conexaoeticacarrefour.com.br or Telephone: 0800 772 2975

The confidential channel - *Conexão Ética* is managed by an external and independent company, guaranteeing the whistleblower in good faith absolute secrecy and non-retaliation. All communication, to the extent permitted by law, will be treated confidentially, with all forms of retaliation against whistleblowers in good faith being prohibited.

9. REVISION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
8/31/2020	01	Policy Drafting	Privacy and Data Protection
7/30/2021	02	Inclusion of DPO's Contact (chapter 5.4) - Inclusion of Link to Privacy Center (chapter 5.4) - Inclusion of Associated Documents (chapter 6)	Privacy and Data Protection

GRUPO CARREFOUR BRASIL

8/21/2023	03	Layout review, text arrangement and inclusion of topic 4.5 Personal data governance	Internal Controls and Privacy and Data Protection
3/19/2025	04	Update of item 4.4: The name of the Data Protection Officer (DPO) has been updated to Thiago Roberto Faria Lima.	Privacy and Data Protection

10. RESPONSIBLE FOR THE DOCUMENT

RESPONSIBLE	VERSION	NAME	AREA	POSITION
Elaboration	04	---------	Privacy and Data Protection	Analyst
Approval	04	---------	Privacy and Data Protection	Manager
Approval	04	---------	Legal	Director
Approval	04	---------	Executive Committee	----------