| Title | PRIVACY AND DATA PROTECTION | Code | PLT_017 |
|---|---|---|---|
| VP/Board | VP of Risks, Compliance, Prevention and Security | Version | 06 |

## Revision History

| Version: | Approval Date: | History: |
|---|---|---|
| 01 | 26/06/2015 | Preparation of the Document. |
| 02 | 07/07/2017 | Inclusion of item IV. Concepts and Acronyms and sub-item 1.1.10 of item VI. Guidelines;<br>Update of items II. Scope, III. Supplementary Documentation and V. Responsibilities. |
| 03 | 29/10/2019 | Update of items II. Scope, III. Guidelines sub-items 1.1, 1.3, 2.4, 2.5, 3.1, 4.1, 5.1 and 6.1, V. Responsibilities, VI. Supplementary Documentation, VII. Concepts and Acronyms and VIII. General Provisions;<br>Inclusion in item III. Guidelines of sub-items 4.2, 4.3 and 4.4. |
| 04 | 29/04/2020 | Update of items I. Purpose, II. Scope, III. Guidelines of sub-items 1, 1.1, 2, 2.1, 2.2, 2.2.1, 2.2.2, 2.3, 3, 3.1, 4, 4.1, 5, 5.1, 6 and 6.1, IV. Consequence Management, V. Responsibilities, and VIII. Concepts and Acronyms.<br>Inclusion of items 1.1.1, 1.1.2, 1.1.3, 1.1.4, 2.1.1, 2.1.2, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8, 3.3, 3.4, 3.5, 5.2, 5.3, 5.4, 7 and 7.1 in item III. Guidelines.<br>Exclusion of sub-items 1.2, 1.2.1, 1.2.2, 1.3, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.4, 2.5, 4.2, 4.3 and 4.4 from item III. Guidelines. |
| 05 | 25/05/2022 | General Document Update. |
| 06 | 09/13/2023 | Update of items I. Purpose, II. Scope, III. Guidelines subitems 1.1.2, 1.1.3, 1.1.4, 2.1.1, 2.1.2, 3.1.1, 3.1.1, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 4.1, 4.4, 4.5, 5.1.4, 5.3, 5.4, 5.5, 6.1, 6.2, 6.4, 6.8, 6.10, 7.1, 7.2, 7.3, 7.4, 8.1, IV. Consequence Management, V. Responsibilities, VI. Supplementary Documentation and VII. Concepts and Acronyms. |

## Table of Contents

## I. Purpose

The purpose of this Privacy and Data Protection Policy ("Policy") is to provide guidance on the guidelines applicable to the privacy and protection of the personal data of customers, employees, third parties, service providers, suppliers and partners to whom Cielo S.A. - Instituição de Pagamento has access as a result of its activities, establishing the rules on the collection, use, storage, sharing and elimination of personal data, in accordance with the laws, regulations and best market practices.

## II. Scope

All members of the Board of Directors, Advisory Committees and Executive Board ("Directors"); members of the Fiscal Council; employees, including outsourced workers, interns and young apprentices ("employees") of the companies Cielo S.A. - Instituição de Pagamento ("Cielo"), Servinet Serviços Ltda. and Stelo S.A., hereinafter jointly referred to as "Company"All members of the Board of Directors, Advisory Committees and Executive Board ("Managers"), members of the Fiscal Council and employees, regardless of position or role held, of the companies Cielo S.A. - Instituição de Pagamento, Servinet Serviços Ltda., Aliança Pagamentos e Participações Ltda. and Stelo S.A., hereinafter referred to as the Company, as well as third parties, service providers and/or suppliers who have access to personal data of these companies.

All the Company's Subsidiaries must define their directions based on the guidelines set forth in this Policy, considering the specific needs and the legal and regulatory aspects to which they are subject.

With respect to the Affiliates, the Company's representatives who act in managing its Affiliates must make every effort to define their directions based on the guidelines set forth

in this Policy, considering the specific needs and the legal and regulatory aspects to which they are subject.

## III. Guidelines

### 1. Initial Provisions

1.1. This Policy aims to demonstrate the Company's commitment to:

1.1.1. Ensure the privacy and protection of personal data collected from customers, employees, third parties, service providers, suppliers and partners, based on the performance of their activities.

1.1.2. Adopt guidelines that ensure broad compliance with laws, regulations and best practices regarding personal data protection.

1.1.3. Promote transparency with data subjects and other stakeholders about how the company processes personal data.

1.1.4. Adopt effective and preventive measures to protect personal data in relation to the risk of security incidents involving such data.

### 2. Information subject to the Policy

2.1. The following are subject to this Policy:

2.1.1. All personal data provided or collected in the context of the provision of services by the Company to its customers for acceptance of e-payments, including the capture, transmission, processing of information and settlement of transactions, as well as the provision of other services and related products.

2.1.2. All personal data of employees, third parties, service providers, suppliers and partners provided or collected in the context of contractual, legal or regulatory obligation or any other personal data.

### 3. Personal data collected

3.1. The personal data collected may vary according to the relationship maintained with the Company and are classified into the following groups:

3.1.1. **Personal data provided by the subject:**Data entered or forwarded by the data subject or his/her legal representative, arising from the contact, registration or contract with the Company, which may include, but not limited to, the following data: full name, CPF [Individual Taxpayer Registry Number], date of birth, marital status, nationality, place of birth, names of parents, beneficiaries, profession, information about the company he/she is a partner, owner, legal representative, or agent, full address, bank information, email address, phone number, and biometric data.

3.1.2. **Personal Data collected from the use of the services:** Data related to the use of electronic payment methods, captured by the Company and transmitted and/or shared with third parties in the context and limit

necessary for the processing and settlement of electronic payment transactions or for the transmission of non-financial information, object of service provided by the Company.

3.1.3. **Personal data collected from the use of websites and applications**: Data related to access and browsing on the Company's website, pages and applications, containing information on device identification (Date, Time and IP). Geolocation of the data subject may also be collected to prevent fraud and security and credit protection.

3.1.4. **Personal Data collected on social media and networks**: Data collected from interactions made by the holders of personal data through the Company's social media and/or networks.

3.1.5. **Personal financial data:** Data concerning the financial or credit status of the subject, such as income, equity, delinquency, credit rating, and data from the Central Bank's Credit Information System, in accordance with applicable legislation in force.

3.1.6. **Personal data of children under 18:** The Company will only collect and process the personal data of minors under the age of 18 under the terms of article 14 of Law 13709/2018 and pursuant to applicable laws.

## 4. Method and purpose of collection

4.1. The personal data will be collected through ethical and legal means and stored in a secure and controlled environment, for the period required by applicable law or regulation. The Company agrees to take all reasonable measures to maintain absolute and strict confidentiality of all personal data to which it has access or that it may be aware of or gain knowledge regarding transactions, holders, data on cards and payment methods, from its customers, as well as individuals directly related to the customers, to which it gains access due to the provision of services by Company, employment, contractual or partnership relationship, being prohibited to assign and/or allow access by third parties to such information, except in the cases described in this Policy and determined by law.

4.2. The Company uses all information collected by filling out the registration, added by the user on its website or app, collected directly from customers or automatically, for the following purposes: (i) provision of services; (ii) expand offers for marketing and dissemination of products and services of interest to customers, employees and partners; (iii) customize and improve products and services offered; and (iv) prevent fraud and financial losses, among other cases that may deviate from conventional practices.

4.3. In some cases, the Company may also process personal data when necessary for compliance with legal or regulatory obligations or regular exercise of rights in judicial, administrative or arbitral proceedings.

4.4. The Company may also process personal data on the basis of its legitimate interest, always within the limits of the expectations of the data subject, and never to the detriment of the interests, rights and fundamental freedoms of the data subject.

4.5. The Company may process sensitive personal data for fraud prevention or research purposes, in which case anonymization will be guaranteed whenever possible. In addition, you may process this data with the consent of the subject.

4.6. The information collected may also be used for advertising purposes, such as for sending communications and news that are of interest to current and potential customers, and to third parties. In such cases, the goal will be to better serve the target audience by offering products that fit their needs and profile.

4.7. The information collected may also be used for profile analysis, identification, management and handling of potential risks then offering and contracting products and/or services and other risk management activities, also aiming at the safety of customers and users.

The data may also be used for the analysis of activities related to credit protection, such as risk assessment and management and assessment of financial

and equity status, collection, credit assignment, activities related to the information and consultation to credit protection entities and credit rating score.

4.8. Also for the fulfillment of legal, regulatory and self-regulatory obligations, such as: auditing, compliance, prevention of money laundering and terrorist financing, reporting to the Internal Revenue Service, fraud prevention measures, providing information to the Central Bank of Brazil and other competent bodies in Brazil and abroad, reporting suspicious transactions to COAF (Financial Activities Control Council), among other activities.

## 5. Relationship with third parties

5.1. The access of third parties to the information collected by the Company is solely for the fulfillment of the purposes set out in this Policy and within the necessary limits for the performance of activities related to the course of its business, and may be carried out, including, but not limited to:

5.1.1. Payment arrangement providers and members of such arrangements;

5.1.2. Electronic funds transfer networks;

5.1.3. Clearing and settlement banks;

5.1.4. Service providers that perform commercial and/or information processing operations for the Company and/or activities related to the Company's activities and that have been subcontracted by the Company;

5.1.5. Marketing Area Partners;

5.1.6. Independent auditors;

5.1.7. Collection agencies, credit protection services and similar bodies; and

5.1.8. Competent regulatory bodies.

5.2. The use of the information collected by the Company, in any of the cases set out in item 5.1 above, is made exclusively to meet the purposes set forth in this Policy, in the performance of the Company's activities or in offering to the client specific content from the use of the information in a secure and comprehensive manner

about its area of operation, in an encrypted manner whenever possible and anonymously when appropriate.

5.3. The Company may share aggregate information with its partners, provided that such information is not personally identifiable. For example, it may share information to demonstrate trends about the general use of its services and/or market trends and indicators.

5.4. Whenever it is necessary to use the information collected for purposes other than those defined in this Policy or those expressly authorized by the data subject, the Company will directly inform the data subject about this new purpose and, when necessary, will collect a new authorization.

5.5. Additionally, it is possible that some of the transfers indicated above may occur outside the Brazilian territory. Destinations can be: United States and the European Union, on which occasion the Company undertakes to do so only for countries that provide a degree of protection for your personal data considered adequate under the applicable legislation; or through the adoption of guarantees and safeguards such as specific clauses, standard clauses, global corporate standards, among others; as well as through the prior collection of your consent or compliance with the other hypotheses authorized by law.

5.6. The Company requires all third parties to maintain the confidentiality of the information shared with them or to which they gain access based on the exercise of their activity, as well as to use such information exclusively for the purposes expressly permitted. However, the Company shall not be liable for the misuse of such information, either by third parties or their employees, due to non-compliance with this Policy and contractual obligations assumed through its own instruments.

5.7. The Company also requires all third parties contracted by it to comply with all obligations contained in this Policy, and the third parties will be subject to the same obligations as the Company, for the data processing activities performed, before the data subjects.

## 6. Information security

6.1. In order to ensure the security of the information collected and/or provided, the Company has physical, logical, technical and administrative security processes that are compatible with the sensitivity of the information collected, the efficiency of which is periodically assessed by means of an independent audit process.

6.2. The Company implements new procedures and continuous technological improvements to protect all personal data collected and/or transmitted.

6.3. The Company uses the latest methods and equipment available on the market to encrypt and anonymize personal data when necessary. Encryption allows us to protect data before it is transmitted over the internet. Encryption techniques make this information unreadable and prevent others from viewing it before reaching our technology environment.

6.4. The Company only authorizes the access of specific persons to the place where the personal information is stored, provided that this access is essential, necessary and essential for the accomplishment of the intended activity.

6.5. The Company guarantees that employees, third parties or partners who process personal data must undertake to maintain the absolute confidentiality of the information accessed, as well as to adopt the best practices for handling this information, as established in the internal policies and regulations.

6.6. In addition to technical efforts, the Company also adopts institutional measures aimed at the protection of personal data, so that it maintains a privacy governance program applied to its activities and structure.

6.7. Access to the information collected is restricted to employees and authorized persons. Anyone misusing this information will be subject to the appropriate administrative, disciplinary and legal sanctions.

6.8. Notwithstanding the security measures adopted, the Company shall not be liable for damages arising from security breaches and/or incidents due to the occurrence of any fact or situation for which it is not responsible.

6.9. When processing the information collected, the Company uses structured systems to meet the security and transparency requirements, good practice and governance standards, and the general principles established in Law No. 13709/2018, the General Personal Data Protection Law ("LGPD").

6.10. The Company has implemented the Information Security and Privacy Management System ("SGSPI"), for the scope established in a specific document, considering the regulatory requirements of ABNT NBR ISO/IEC 27001:2022 and ISO/IEC 27701:2020 and the robust governance structure already in place at the Company. The process is structured in the model of continuous improvement, providing constant evolution of information security and privacy issues and aligned with the guidelines established in this Policy. The definitions on the matter, as well as the roles and responsibilities, are formalized in the Security and Privacy Management System Handbook.

## 7. Rights of data subjects

7.1. In compliance with the applicable regulations, with regards to the processing of personal data, the Company respects and guarantees to the data subject the possibility of submitting requests based on the following rights:

- Confirmation of the existence of processing;
- Access to personal data;
- Correction of incomplete, inaccurate or outdated information;
- Anonymization, blocking or deletion of data that is unnecessary, excessive or legally noncompliant;
- Portability of the data to another service provider or product, upon express request by the User;
- Deletion of data processed with the User's consent;

- Obtaining information about the public or private entities with which the Company shares their data;
- Information on the possibility of the user not providing consent, as well as being informed about the consequences in case it is denied; and
- Withdrawal of consent; and
- Review of decisions taken solely on the basis of automated processing of personal data.

7.2. Part of the above rights may be exercised directly by the data subject or their legal representative, by managing the registration information available in the logged-in area of the site, while another part will depend on sending a request to the Privacy and Data Protection area, for evaluation and adoption of the necessary measures. The channel for receiving requests of this nature is the email: privacidade@cielo.com.br.

7.3. For more information, questions or requests regarding the processing of data, please refer to the External Privacy Notice, available at: www.cielo.com.br/privacidade, or contact the Person Data Processing Officer ("DPO"), by email: privacidade@cielo.com.br.

7.4. Any request for deletion of information essential for the management of registration with the Company will imply the termination of its contractual relationship, with the consequent cancellation of the services then provided, and the data may be kept to comply with legal or regulatory determination.

## 8. Cooperation with regulatory authorities

8.1. In the event that it becomes necessary to disclose personal data, whether due to compliance with the law, a court order or a competent body supervising the activities carried out by the Company and/or third parties, such information shall only be disclosed in the strict terms and within the limits required for its disclosure, and the holders of the information disclosed shall, as far as possible, be notified of such disclosure, so that they may take appropriate protective or remedial measures.

## 9. Amendments

9.1. This Policy may be amended at any time, depending on the purpose or need for adequacy and compliance of the provision of law, regulation or whenever the Company deems necessary. Changes will be disclosed through the websites https://www.cielo.com.br/ and https://ri.cielo.com.br/. The continued use of the services or the provision of services to the Company, as the case may be, after disclosure of the changes, will be considered acceptance of the client and third parties regarding the new terms and conditions.

# IV. Consequence Management

Employees, vendors or other stakeholders who observe any deviations from the guidelines of this Policy may report the fact to the Ethics Channel through the channels below, with the option of anonymity:

- www.canaldeetica.com.br/cielo
- Toll-free number: 0800 775 0808

Internally, non-compliance with the guidelines of this Policy gives rise to the application of accountability measures to the agents that fail to comply with it, according to the respective severity of the non-compliance and as per internal regulations, and is applicable to all persons described in the item "Scope" of this Policy, including the leadership and members of the Executive Board.

When an incident reported to the Ethics Channel involves personal data and/or sensitive personal data, the area responsible for the Ethics Channel must promptly report the complaint to the Personal Data Processing Officer ("DPO").

## V. The definition of relevance of incidents in the technological environment follows the corporate standard of risks established in internal standard NRM_124 Non-Financial Risk Management.

- **Officers, Employees and Service Providers:** Observe and ensure compliance with this Policy and, when necessary, to contact the Personal Data Processing Officer for guidance on situations involving conflict with this Policy or upon the occurrence of situations described therein. Act ethically and responsibly when becoming aware of any security incident involving personal data, informing, in a timely manner, the appropriate areas. Understand the role of information security and privacy in their daily activities and participate in awareness and education programs, as well as contribute to the implementation, maintenance and continuous improvement of the SGSPI.
- **Vice Presidency of Risks, Compliance, Prevention and Security:** Complying with the guidelines established in this Policy, keeping it up to date in order to ensure that any legal and/or regulatory changes or new Company guidelines are incorporated and clarifying doubts regarding its content and application.
- **Privacy and Data Protection:** Advising the Executive Board on privacy and data protection issues, with a view to compliance with applicable laws and regulations, in particular Law No. 13709/2018, the General Personal Data Protection Law. Forum members must promote the relevance of the SGSPI in the company, acting as ambassadors for the subject in their respective areas, as well as carrying out periodic critical analysis of the system and other related activities.
- **Executive Board:** Deliberate, as recommended by the Privacy and Data Protection Forum, on the resources for the implementation, maintenance and improvement of the Information Security and Privacy Management System, including conducting periodic critical analysis of the system, appreciating the results, metrics and indicators, as well as promoting the relevance of the SGSPI for all employees.
- **Vendors**: Observe and ensure compliance with the best practices of information security and privacy, contractually required during the relationship with the Company. Act ethically and responsibly when becoming aware of any security incident involving personal data, and that may entail relevant risks to the holders informing, in a timely manner, the appropriate areas.

- **Vice-Presidency of Legal and Government Relations:** Answer any questions on laws and regulations that apply to the subject described in this Policy.

## VI. Supplementary Documentation

- Article 5 of the Federal Constitution of 1988;
- Company Code of Ethics;
- Cielo Accreditation Contract;
- Supplementary Law No. 105/2001;
- Law No. 12965 dated April 23, 2014 - Internet Civil Framework.
- Law No. 13709 dated August 14, 2018 - General Data Protection Law ("LGPD").
- ABNT NBR ISO 27001 - Information Security.
- ABNT NBR ISO 27701 – Information Privacy;
- Internal Regulations of the Privacy and Data Protection Forum; and
- Internal standards that are constantly improved, approved by the competent approval authority, and provided to all employees.

## VII. Concepts and Acronyms

- **Clients:** Individual who has registered in the Company's system, to whom the personal data that are the object of work refer;
- **Personal data:** Any information related to the identified or identifiable individual, such as: first name, last name, date of birth, personal documents (CPF [Individual Taxpayer Registry], RG [ID], CNH [Drivers License], Employment Record Card, passport, voter registration card, among others), home or business address, phone, email, cookies and IP address;
- **Sensitive personal data:** Any personal data on racial or ethnic origin, religious belief, political opinion, membership to a trade union or religious, philosophical or political organization, data concerning health or sexual life, genetic or biometric data, when linked to an individual;
- **Personal Data Processing Officer ("DPO"):** Person appointed by the Company to serve as a point of contact between the personal data subjects and the National Data Protection Authority ("ANPD"), as well as in charge of the initiatives of the Company's Data Privacy Governance Program.
- **Information:** Data, processed or not, that can be used for production and transmission of knowledge, contained in any medium or format;
- **Protection of Personal Data:** Guarantee to data subjects the rights of access, correction, control and confidentiality of information.
- **SGSPI:** Sistema de Gestão de Segurança e Privacidade da informação.

- **Affiliates:** Companies in which the Company holds 10% (ten percent) or more of their capital, without, however, controlling them, under the terms of article 243, paragraph 1 of the Brazilian Corporation Law.
- **Subsidiaries:** Companies in which the Company, directly or indirectly, holds partner or shareholder rights that assure it, on a permanent basis, preponderance in the corporate decisions and the power to elect the majority of the managers, under the terms of article 243, paragraph 2 of the Brazilian Corporation Law.
- ***Stakeholders*:**All relevant target audiences with interests pertinent to the Company, as well as individuals or entities that assume some type of risk, direct or indirect, with respect to the company. Among others, the following are highlighted: shareholders, investors, employees, society, clients, vendors, creditors, governments, regulatory bodies, competitors, press, associations and class entities, users of electronic means of payment, and non-governmental organizations.
- **Third parties:** Individual or legal entity, public or private, who provides services to the Company, on its premises or remotely, and who, in the exercise of their activities, may gain access to information related to the business of the Company or its Clients.
- **Data subject**: Individual to whom the personal data object of processing refer.

## VIII. General Provisions

The Company's Board of Directors is responsible for altering this Policy whenever necessary.

This Policy takes effect on the date of its approval by the Board of Directors and revokes any documents to the contrary.

Barueri, September 13, 2023.

**Cielo S.A. – Instituição de Pagamento**