PRIVACY AND PERSONAL DATA PROTECTION POLICY

Papirus Indústria de Papel S/A is committed to protecting the privacy of its employees and all other individuals involved in its operations. This Policy sets forth our commitment to safeguarding personal data in compliance with the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais – LGPD, Law No. 13,709/2018) and all other applicable data protection legislation, and describes how your privacy is protected in the collection, processing, and storage of personal information.

This Policy governs how personal information required for the Company's operations is collected through physical and electronic means, the lawful purposes for which it is used, and how it is processed and transferred.

Papirus Indústria de Papel S/A operates under its own Code of Conduct, grounded in its corporate values. Each principle set forth in the Code reflects the Company's commitment to safety, quality, and ethical conduct in its relationships with employees and all other stakeholders. The Code was developed to promote transparent and ethical business practices, respect for people and the environment, and to build lasting, mutually beneficial relationships with all parties involved.

Accordingly, Papirus Indústria de Papel S/A, hereinafter referred to as the "Controller", registered with the Brazilian Federal Taxpayers' Registry (CNPJ) under number 60.856.077/0001-90, with its registered office at Rodovia Anhanguera, km 130, Jaguari district, Limeira, State of São Paulo; a branch and production facility also located at Rodovia Anhanguera, km 130, Jaguari district, Limeira, State of São Paulo, registered under CNPJ number 60.856.077/0009-47; and a branch and commercial office at Av. Santo Amaro, 3,330, 6th floor, Brooklin district, São Paulo, State of São Paulo, registered under CNPJ number 60.856.077/0009-66 — acting in its capacity as Data Controller — is bound by the provisions of this Privacy Policy.

1. Definitions

Data Subject / Individual: Any natural person who maintains a relationship with the Company, whether as an employee, client, supplier, outsourced worker, partner, shareholder, or any other individual who is required to provide personal data as a condition of interacting with or conducting any activity, work, service engagement, or visit.

Personal Data: Any information provided and/or collected by the Controller, by any means, that: (i) identifies, or that, when used in combination with other information processed by Papirus Indústria de Papel S/A, identifies a natural person; or (ii) from which the identification or contact details of a natural person can be derived. Personal Data may exist in any medium or format, including electronic or computerized records and paper-based files. Personal Data does not include corporate telephone numbers, corporate mobile numbers, corporate addresses, or corporate email addresses.

Processing Purpose: The specific objective or end for which the Controller processes personal information in each particular instance.

Table of Purposes (Purpose Register): A structured register presented in tabular format to explain, in a clear, organized, and transparent manner, what personal data the Company retains, how it is processed, and the legal basis for such processing.

Necessity: The principle requiring that the collection of personal data be strictly limited to what is necessary to achieve the specified purpose, so as to avoid the collection of excessive or irrelevant data.

Legal Basis: The legal ground that authorizes the Controller to process personal data for a specific and predetermined purpose, independently of the data subject's consent, including grounds arising from applicable legislation or a collective bargaining agreement.

2. Consent

Consent is the freely given, informed, and unambiguous expression of will by which the data subject authorizes the Controller to process their personal data for a specified purpose.

Accordingly, and in compliance with the LGPD, your personal data will only be collected, processed, and stored upon receipt of your prior and express consent.

Consent will be obtained specifically for each processing activity, reflecting the Company's commitment to transparency and good faith in its dealings with data subjects, in accordance with applicable legislation.

You may withdraw your consent at any time, free of charge. It is important to note that withdrawal of consent for certain processing activities may render the provision of particular services, benefits, or participation in selection processes and other activities unfeasible.

Any such consequences will be communicated to you at the time your withdrawal request is received.

2.1 What are your rights?

The Controller ensures that data subjects may exercise all rights recognized under Article 18 of the LGPD. You may, free of charge and at any time:

- Confirm the existence of processing of your personal data, in simplified or in complete and clear format;
- Access your personal data, by requesting a legible hard copy or access through secure and reliable electronic means;
- Request the correction of incomplete, inaccurate, or outdated data;
- Request the anonymization, blocking, or deletion of unnecessary, excessive, or unlawfully processed data;
- Request the deletion of personal data processed on the basis of your consent, subject to the exceptions provided by law;
- Revoke your consent at any time, thereby withdrawing your authorization for the processing of your personal data;
- Obtain information about the possibility of refusing consent and the consequences of such refusal.

2.2 How can you exercise your rights as a data subject?

To exercise your rights as a data subject, you may contact the Controller through any of the following channels:

- HR Department: contact the Company's Human Resources department directly;
- Website: www.papirus.com — use the contact form to submit your details and message;
- Telephone: +55 (19) 2113-6148 — contact Thaís Barros;
- E-mail: ouvidoria@papirus.com

In order to verify your identity as the data subject making the request, the Controller may require you to provide documentation or other proof of identity. You will be informed in advance should such verification be necessary.

By accessing and/or using the Papirus Indústria de Papel S/A website, the User represents that they are at least 18 (eighteen) years of age and/or have full legal capacity to accept the terms and conditions of this Privacy Policy and the associated Consent Form, for all legal purposes.

If the data subject does not agree, even in part, with the terms and conditions set forth in this Privacy Policy, they must expressly declare so in order to terminate the relevant relationship with the Company.

The data subject acknowledges that they are providing information consciously and voluntarily through forms, document copies, and other means, including through websites operated by Papirus Indústria de Papel S/A.

When a data subject registers or completes forms made available by Papirus Indústria de Papel S/A — including those available on the Company's operated websites — the personal data requested will be kept confidential and used solely for the purpose that justified the collection, as set forth in the Table of Purposes.

Papirus Indústria de Papel S/A will not make personal data available for any purpose other than those disclosed, without the express consent of the data subject or without a valid legal basis or purpose as reflected in the Table of Purposes.

The Controller may disclose collected personal data to third parties in the following circumstances, within the limits permitted and required by law:

I. To clients and business partners, where necessary and/or appropriate for the provision of associated services;
II. To subsidiaries and affiliated companies;
III. To service providers and partners engaged to perform services contracted with Papirus Indústria de Papel S/A (such as providers of meal vouchers, food vouchers, transportation vouchers, health insurance, pharmacy benefits, and other employer-sponsored benefits);
IV. For administrative purposes, including research, planning, service development, security, and risk management;

V. Where required by law, by order of a competent authority, or by court order.

In all cases where personal data is shared with third parties, the parties listed above must use such data in a manner consistent with the purposes for which it was originally collected (or to which the data subject previously consented), and in accordance with the provisions of this Privacy Policy.

3. How and for how long will your data be stored?

Personal data collected by the Controller will be used and retained for the period necessary to fulfil the purpose for which it was collected or to provide the relevant service, as described in this Privacy Policy, and in accordance with the rights of data subjects and controllers.

As a general rule, your personal data will be retained for as long as the contractual relationship between you and the Controller subsists. Upon expiry of the applicable retention period, personal data will be deleted from our databases or anonymized, except in the circumstances provided for in Article 16 of the LGPD, namely:

I. Compliance with a legal or regulatory obligation by the Controller;
II. Research conducted by a public authority or research body, provided that anonymization is ensured wherever possible;
III. Transfer to a third party, in compliance with the data processing requirements established by the LGPD; or
IV. Exclusive use by the Controller, in anonymized form, with access by third parties prohibited.

Personal data that is essential for compliance with legal, judicial, or administrative obligations, or for the exercise of the right of defense in judicial or administrative proceedings, will be retained notwithstanding the deletion of other data.

We employ technical protection measures designed to ensure the confidentiality, integrity, and inviolability of your data. In addition, we also

have security controls in place that are appropriate to the risks involved and govern access to stored information accordingly.

4. What we do to keep your data safe;

To protect your personal information, we apply physical, electronic, and administrative safeguards designed to preserve your privacy.

These measures are implemented taking into account the nature of the personal data collected, the context and purposes of the processing, and the risks that any breach could pose to the rights and freedoms of the individuals whose data is processed.

Among the measures we have adopted, we highlight the following:

- Access to your personal data is restricted to authorized personnel only;
- Access is granted only after authorized individuals have executed a confidentiality agreement and/or a data processing agreement with relevant third parties;
- Your personal data is stored in a secure and reliable environment.

Papirus Indústria de Papel S/A is committed to adopting best practices to prevent security incidents. However, it is important to note that no website or information system is entirely free from risk. It is possible that, despite all our security protocols, problems attributable to third parties may occur, such as cyberattacks by malicious actors, or resulting from negligent or reckless conduct by the user.

In the event of a security incident likely to result in significant risk or harm to any individual, the Controller will notify the affected data subjects and the National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD) in accordance with the LGPD.

5. Who your data may be shared with;

In order to protect your privacy, the Controller will not share your personal data with unauthorized third parties.

Your personal data may be shared with our business partners in accordance with the terms of applicable commercial agreements.

Such partners receive your data solely to the extent necessary for the provision of contracted services. All data processing arrangements are governed by the data protection requirements of Brazilian law.

Please note that our partners maintain their own privacy policies, which may differ from this one. We recommend consulting those documents, which may be requested at any time.

In addition, there are other circumstances under which your data may be shared, which are:

I. By determination, order, or decision of competent judicial, administrative, or governmental authorities; legal, application, request or order judicial, with the competent judicial, administrative or governmental authorities.
II. In the context of corporate transactions, such as mergers, acquisitions, or consolidations, on an automatic basis;
III. For the protection of the Controller's rights in any type of dispute, including judicial proceedings.

5.1 International data transfer

Where any of the third parties with whom we share your personal data operate servers or facilities located outside Brazil, your data may be subject to international transfer. Under such circumstances, your personal data will continue to be governed by the LGPD and all other applicable Brazilian data protection legislation.

The Controller is committed to maintaining robust cybersecurity and data protection standards at all times, and to ensuring full compliance with applicable legal requirements.

By agreeing to this Privacy Policy, you consent to the international transfer of your data to the extent described herein and for the purposes set forth in this document.

6. Cookies or browsing data

The Controller uses cookies — small text files sent by the platform to your device and stored thereon — which contain information relating to your browsing activity on the website. Cookies are used to enhance the user experience by enabling features such as content personalization, performance analysis, and continuous service improvement.

By accessing our website and consenting to the use of cookies, you acknowledge and accept the collection of browsing data through cookies stored on your device. Further information about the cookies we use is available by clicking the green ‘Consent Preferences’ icon located in the lower left corner of the Company’s official website, where you may configure your preferences accordingly.

7. Changes to this Privacy Policy

The current version of this Privacy Policy was last revised and updated on: May 12, 2026.

The Controller reserves the right to amend this Privacy Policy at any time, particularly to reflect changes to our website or to comply with updates in applicable legislation.

Any amendments will take effect upon publication on the Company’s official website.

8. Responsibility

The Controller recognizes the responsibility of data processing agents in accordance with Articles 42 to 45 of the LGPD.

The Controller is committed to keeping this Privacy Policy current, observing its provisions, and ensuring their effective application.

Furthermore, the Controller undertakes to implement technical and organizational measures capable of ensuring the lawful and secure processing of personal data.

Should the ANPD require the Controller to take any action with respect to the data processing activities described herein, the Controller undertakes to comply in full.

8.1 Disclaimer

As stated above, although the Controller adopts high security standards to prevent incidents, no information system is entirely risk-free. Accordingly, the Controller shall not be liable for:

I – Any consequences arising from negligent, reckless, or careless conduct by the data subject with respect to their own personal data. The Controller warrants only the security of its own data processing activities and the fulfilment of the purposes described in this Policy.
The responsibility for maintaining the confidentiality of access credentials lies with the user.

II – Malicious acts by third parties, such as cyberattacks, except where proven to result from deliberate or culpable conduct attributable to the Controller. The Controller reaffirms that, in the event of a security incident likely to result in significant risk or harm to data subjects, it will notify those affected and the ANPD and take all necessary remedial measures.

III – Inaccuracies in information entered by the user in records required for use of the Controller's services. Any consequences arising from false or bad-faith information are the sole responsibility of the user.

9. Data Protection Officer

The Controller designates a Data Protection Officer (Encarregado de Proteção de Dados) responsible for acting as a communication channel between the Controller, data subjects, and the ANPD, in accordance with Article 41 of the LGPD. You may contact us to exercise your rights as a data subject through the following means:

e-mail: ouvidoria@papirus.com

If you have any questions about this Privacy Policy or the personal data processed by the Controller, you may contact our Data Protection Officer through the following channel:

Ms. Thaís Barros

e-mail: ouvidoria@papirus.com

TABLE OF PURPOSES

PERSONAL DATA	SENSITIVE?	OWNERSHIP	PURPOSE	LEGAL BASIS TREATMENT	TREATMENT PERIOD	TREATED BY SECTOR	TREATMENT METHOD	DATABASE
Full name /CPF/ID	No	Employee (CLT) Outsourced employee and/or self-employed worker	Electronic: eSocial, DIRF, HR system (all modules) / SESMT / General benefits management/ General announcements / Training registrations / Participation in general audits / Legal compliance (legal obligations related to work, taxes and regulations) / Complaint management / Reports and Statistics	Legal obligation (Art. 7, item II, LGPD)	Indefinite term	HR	Physical | Electronic	Senior/Internal Server/DPM Access
Voter registration card	No	Employee (CLT) Outsourced employee and/or self-employed worker	Not defined	Inexistant	Inexistant	HR	Physical | Electronic	Senior/Internal Server/DPM Access
Race / Color	Yes	Employee (CLT) Outsourced employee and/or self-employed worker	Electronic: eSocial, DIRF, HR system (all modules) / SESMT / General benefits management/ General announcements / Training registrations / Participation in general audits / Legal compliance (legal obligations related to work, taxes and regulations) / Complaint management / Reports and Statistics	Legal obligation (Art. 7, item II, LGPD) / consent	Indefinite term	HR / OUTPATIENT CLINIC	Physical | Electronic	Senior/Internal Server/DPM Access
Phone number / Email / Home address	No	Employee (CLT) Outsourced employee and/or self-employed worker	Electronic: eSocial, DIRF, HR system (all modules) / SESMT / General benefits management/ General announcements / Training registrations / Participation in general audits / Legal compliance (legal obligations related to work, taxes and regulations) / Complaint management / Reports and Statistics	Legal obligation (Art. 7, item II, LGPD)	Indefinite term	HR	Physical | Electronic	Senior/Internal Server/DPM Access
Bank account/branch	No	Employee (CLT) Outsourced employee and/or self-employed worker	Process financial information related to salaries and benefits.	Consent	Indefinite term	HR	Physical | Electronic	Senior/Internal Server/DPM Access
Personal Image	No	Employee (CLT)	Personal identification via badge and system / Marketing of Enterprise	Consent	Indefinite term	HR	Physical | Electronic	Senior/Internal Server/DPM access
Full name /CPF/ID	No	Candidate	Resume / Job opening	Consent (Art. 7, item I, LGPD)	minimum 12 months	HR	Physical | Electronic	Senior/Internal Server
Race / Color	Yes	Candidate	Job opening / Possible diversity policy	Consent (Art. 11, item I, LGPD)	minimum 12 months	HR	Physical | Electronic	Senior/Internal Server
Phone number / Email / Home address	No	Candidate	Job opening	Consent (Art. 11, item I, LGPD)	minimum 12 months	HR	Physical | Electronic	Senior/Internal Server
Full name /CPF/ID	No	Dependent	Electronic: eSocial / DIRF / HR system / General benefits management / General communications / Legal compliance (legal obligations related to work, taxes and regulations) / Reports and Statistics	Consent	Indefinite term	HR	Physical | Electronic	Senior/Internal Server
Phone number / Email / Home address	No	Dependent	Electronic: eSocial / DIRF / HR system / General benefits management / General communications / Legal compliance (legal obligations related to work, taxes and regulations) / Reports and Statistics	Consent	Indefinite term	HR	Physical | Electronic	Senior/Internal Server
Full name /CPF/ID	No	Visitor	Electronic: Legal compliance (legal obligations related to work, taxes and regulations) / Reports and Statistics	Consent	Indefinite term	HR	Physical | Electronic	DPM Access/Internal Server