PRIVACY POLICY

Introduction

Snacks Développement SAS known as Europe Snacks Group takes your privacy very seriously and is committed to protecting it. This Privacy Policy explains how Europe Snacks Group and its relevant local entities acting as data controllers collect, use, disclose, and protect your personal data in compliance with the GDPR and applicable local data protection laws, including CNIL guidelines and Ecovadis standards. This Policy applies to all personal data collected via our websites, business relationships, recruitment, site security, and other interactions. We want you to understand how we collect and use information about you. We also value your comments about the way we do this.

The privacy policy describes to you:

- who we are ;
- where this site is hosted ;
- what personal data we collect and store about you, and how we collect it;
- why we collect personal data and what we do with it;
- the categories of third parties with whom we share your personal data;
- how we retain your information and keep it secure;
- how long we keep your personal information;
- which countries we transfer your personal information to;
- your rights and how to exercise them;
- how to contact us.

It also contains information on the correct people to contact in the unlikely event that you have a complaint.

1. Data Controller

Our name: Snacks Développement SAS known as Europe Snacks (but we will refer to ourselves using the word “we” and related words such as “us” and “our” in this privacy policy)
Place of incorporation: France

Company number: 798 741 211

Registered address: ZI Saint Denis les Lucs – 85170 SAINT DENIS LA CHEVASSE

SAS au capital de 63 548 866,39 Euros

VAT number: FR53 798 741 211

Local Europe Snacks entities may act as controllers for processing related to their activities. Contact details for specific controllers are available upon request.

2. Contact Information

For privacy questions or to exercise your rights, contact:

Email: dataprotection@europesnacks.com

Postal address: EUROPE SNACKS, ZI St Denis les Lucs – BP 18, 85170 Saint Denis la Chevasse, France, Attention: Legal Department

If a Data Protection Officer is appointed, their contact details will be provided in relevant notices.

3. Where is this site hosted?

Greenshift S.A.S. 9, rue Campagne Première 75014 Paris France Capital: 20 000 € RCS Paris B 524 234 051 SIRET: 52423405100018 TVA: FR 37524234051 NAF: 6311Z

On Behalf of La Cellule S.A.R.L. (hereinafter Big District) 42 rue Monge 75005 Paris France Capital 20 000€ RCS Paris 539 714 956 TVA FR25 539 714 956

4. Personal Data Collected

We collect:

- personal details, such as name, title, username, gender, date of birth, copy of passport/ID;
- contact data, such as delivery address, billing address, e-mail address, telephone and mobile number(s);
- image data, namely CCTV images ;
- biographical data from job applications and CVs, such as institutions attended, academic and other results gained, employment history, any other personal information you provide;
- payment details, such as bank account, card details;

- transaction data, such as details about payments to and from you, details of products and services you have purchased from us;
- technical data, such as internet protocol (IP) address, login data, browser type and version, time-zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website;
- profile data, such as orders made by you, feedback and survey responses;
- usage data, such as information about how you use our website, products and services;
- marketing data, such as your preferences in receiving marketing and communications;
- security data (CCTV images, access logs);
- supplier and partner data.

We do not knowingly collect "special category" personal data unless strictly necessary, lawful, and with safeguards. This includes data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data and/or biometric data. We also do not collect information about criminal convictions or offences.

5. Sources of Data

We obtain personal data from sources as follows:

- directly from you when you interact with us, for example when you request information, buy our products, write to us, apply for a job, send a CV or start employment with us;
- from others if they provide your details – for example, if a person sends an e-mail to us and copies you on the e-mail, and your e-mail address identifies you by name (please ensure you have that person's consent to do so);
- from automated technologies such as cookies and tags when you use our website.

6. Purposes and Legal Bases

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- to perform a contract we are about to enter into or have entered into with you;
- if it is necessary for our legitimate interests (or those of a third party) and these are not overridden by your own rights and interests;

- where we need to comply with a legal or regulatory obligation. We process data to:
- manage relationships and contracts ;
- process orders and payments ;
- handle recruitment and onboarding ;
- operate and secure our systems and premises;
- prevent fraud and abuse ;
- send communications and marketing with consent;
- comply with legal obligations.

Legal bases include contract performance, legitimate interests (balanced with your rights), legal obligations, and consent where required.

We will use your personal data only for the purposes for which we collected it, unless we fairly consider that we need it for another reason that is compatible with the original purpose.

This Privacy Policy is available in French and Spanish ; in case of discrepancy, please refer to the English version of this Privacy Policy.

7. Do we share your personal data?

We may provide your personal data to the following recipients for the purposes set out in this policy:

- other companies in our group ;
- our service providers, including logistics providers, e-mail and mail service providers, technical and support partners, payroll and employee benefits providers;
- merger or acquisition partners, to the extent that sharing your personal data is necessary;
- law enforcement agencies, government or public agencies or officials, regulators, and any other person or entity that has the appropriate legal authority where we are legally required or permitted to do so, to respond to claims, or to protect our rights, interests, privacy, property or safety;
- any other parties, where we have your specific consent to do so.

8. Do you have to provide personal data – and, if so, why?

To form a contract with you, we will need some or all of the personal data described above so that we can perform that contract or the steps that lead up to it. If we do not receive the data, the contract could not be performed.

9. Data Retention

We carefully consider the personal data that we store, and we will not keep your information in a form that identifies you for longer than is necessary for the purposes set out in this policy or as required by applicable law (i.e. Article 5 of GDPR regulation). In some instances, we are required to hold data for minimum periods. Here below you can find a general global approach on the retention periods per category of data:

- Administrative and identification data: 100 years ;
- Notarial documents: 30 years from completion of formalities;
- Authentic Act and annexes: 75 years ;
- Authentic Act concerning protected minors or adults :respectively, 100 years and 75 years from the completion of the formalities ;
- Job Candidate data: 1 year ;
- Customer data (active commercial relationship): Duration of the contractual relationship + 5 years;
- Prospect data: 2 to 3 years from last incoming contact;
- Data collected for cybersecurity: 2 to 10 years depending purpose;
- Money laundering and terrorist financing checks: 1 year from last use;
- Traceability and safety data: 13 months for computer traces;
- Electronic identification data: 6 years from last use;
- Fraud and litigation data: Unqualified fraud alerts: Maximum 12 months from issue date Qualified fraud alerts: 5 years from the closure of the file Fraud list registration: 5 years from the date of registration
- Data relating to legal proceedings: Until the end of the procedure + limitation period (5 years);
- Data relating to exercise rights demands: 1 year to 6 years depending on the right exercised;
- Data linked to consent (cookies): 6 months for selection, 25 months for data;
- Cookies and consent records: as per Cookie Policy;
- CCTV and security logs: minimum necessary period per site security procedures Data is securely deleted or anonymised after retention.

10. Cookies and Similar Technologies

We use cookies to operate websites, measure performance, and, with your consent, for marketing and analytics. Non-essential cookies are deployed only after clear consent, which you may withdraw anytime via cookie settings or browser controls. Our detailed Cookie Policy, including cookie categories, purposes, retention periods, and opt-out options, is available at https://www.europesnacks.com/cookies-policy/ .

Among the solutions that have been certified as compliant with GDPR regulations by the French local authority named Commission Nationale de l'Informatique et des Liberté's (CNIL) during its assessment, Europe Snacks selected Matomo Analytics which as well as minimising the collection of personal data, Matomo automatically takes measures to protect privacy, such as updating users' digital fingerprints daily so that user profiles cannot be built up over time. You may refuse to have your browsing on this Website tracked. This will protect your privacy, but will also prevent the owner from learning about your actions and creating a better experience for you and other users.

11. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorized access, alteration, disclosure, or destruction. Access to sensitive data such as CCTV footage is strictly limited to authorized personnel under confidentiality obligations. We have security measures in place designed to prevent data loss, to preserve data integrity, and to regulate access to the data. Only our authorised employees and third parties processing data on our behalf have access to your personal data.

We also maintain an up-to-date internal register of all our data internal processing and external processors, which identifies for each of them the categories of personal data processed, the purposes and means of processing, as well as the relevant retention periods. This register is reviewed and updated on a regular basis to ensure that our use of data processors remains compliant with applicable data protection law, including the GDPR.

All our employees who have access to your personal data are required to adhere to our Privacy Policy and we have in place contractual safeguards with our third-party data processors to ensure that your personal data is processed only as instructed by us.

We take all reasonable steps to keep your data safe and secure and to ensure the data is accessed only by those who have a legitimate interest to do so. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us. Any transmission is at your own risk. Once we have received your personal data, we will use strict procedures and security features to try to prevent unauthorised access.

12. International Transfers

Although we are based in France, we may transfer your personal information to a location (for example, to a secure server) outside the European Economic Area, if we consider it necessary or desirable for the purposes set out in this policy.

In such cases, to safeguard your privacy rights, transfers will be made to recipients to which a European Commission "adequacy decision" applies (this is a decision from the European Commission confirming that adequate safeguards are in place in that location for the protection of personal data), or will be carried out under standard contractual clauses that have been approved by the European Commission as providing appropriate safeguards for international personal data transfers.

13. Your Rights

Subject to applicable law, you have the right to:

- be informed about data processing ;
- access your personal data ;
- request correction or deletion ;
- restrict or object to processing ;
- withdraw consent at any time ;
- receive data portability where applicable;

To exercise your rights, contact dataprotection@europesnacks.com with sufficient information to identify you. We may request identity verification.

These rights are subject to certain limitations that exist in law. Further information about your information rights is available on the CNIL's, the ICO's and the AEPD's websites.

14. Consent of Minors

Where applicable, we obtain parental or guardian consent before processing personal data of minors, in compliance with local laws.

15. Additional Information and Updates

This Policy may be updated to reflect legal or operational changes. Material changes will be communicated via our website or other channels. The “Last updated” date will be revised accordingly.
For specific processing activities covered by separate local notices or contracts, these documents should be consulted alongside this Policy. Access to such documents is available upon request.

The policy indicates that other local documents may prevail, but does not specify how the user can easily access them; access is available upon request.

16. Complaints

If you have concerns about data processing, please contact us first. You also have the right to lodge a complaint with the relevant supervisory authority (e.g., CNIL, ICO, AEPD).

17. Internal Governance

Our privacy governance includes documented procedures for processing records, retention, access control, incident response, supplier due diligence, and rights management. These are regularly reviewed to ensure compliance with GDPR, CNIL guidance, and Ecovadis standards.

18. Dates

Effective date: 21/05/2026

Last updated: 21/05/2026