Privacy Policy — notice under artt. 13 and 14 GDPR

Controller	[Legal name of owner]
VAT Number	[VAT Number]
Registered office	[Office address]
Contact	[Support email]
Website	www.smoves.it
Last updated	[Last update date]

Table of contents

1. Data controller and contacts

1.1 The data controller is [Legal name of owner], sole proprietorship, VAT Number [VAT Number], with registered office at [Office address] (hereinafter, "Controller" or "Smoves").

1.2 Contact email for the exercise of rights and privacy matters: [Support email].

1.3 The Controller has not appointed a Data Protection Officer (DPO), since the requirements of art. 37 GDPR are not met (absence of large-scale processing of special categories of data, systematic monitoring and public authority activities). The appointment may be made in case of changes in operating conditions.

2. Categories of data processed

2.1 Smoves processes, including through automated tools, the following categories of personal data:

identification and contact data: name, surname, email address, telephone number, data of any representatives or referents;

logistical and operational data relating to the Service: collection, storage and delivery addresses, geographic coordinates, times, operational instructions, notes entered by the Data Subject;

administrative, tax and invoicing data: tax code, VAT number, billing address and further data required by applicable law;

payment and anti-fraud data: metadata relating to transactions, payment identifiers, outcome of operations, anti-fraud and risk verification information provided by payment providers;

data relating to packages and stored items: photographs, videos, recordings of the external state of the package, of the seal and of the packaging, description of the content, declared value, any anomalies detected;

data relating to use of the Service: booking history, interactions with customer service, tickets, complaints, feedback and communications;

technical and navigation data: IP address, device ID, browser, operating system, language, date and time of access, application and telemetric logs;

data deriving from security checks, fraud prevention, operational risk management and

judicial protection.

2.2 Smoves does not request and does not intentionally process special categories of personal data (art. 9 GDPR). The Data Subject is invited not to enter such data in non-necessary communications.

2.3 Smoves reserves the right to carry out checks on the accuracy, completeness and consistency of the data provided by the Data Subject, including through automated controls, where necessary for security, fraud prevention, operational risk management, protection of company assets or prevention of abusive use of the Service.

3. Purposes and legal bases of processing

3.1 Personal data are processed for the following purposes:

execution of the contract and operational management of the Service;

verification of the Data Subject's identity and prevention of fraudulent, abusive or contractual-breach use;

protection of the rights, security and assets of the Controller, logistics partners and third parties;

management of disputes, debt collection, litigation and out-of-court or judicial activities;

monitoring of Service quality, commercial development, statistical analysis, improvement of internal processes and operational optimisation;

prevention of unlawful conduct, damage, theft, loss or improper use of the Service;

compliance with obligations provided by national and European law;

sending of commercial, informational and promotional communications relating to services similar to those already purchased by the Data Subject, pursuant to art. 130, paragraph 4, of Italian Legislative Decree 196/2003 ("soft spam"), subject to opt-out;

sending of marketing communications and newsletters subject to consent, where required;

management of extraordinary corporate transactions, due diligence, transfer of business, branches of business or assets.

3.2 Processing based on the legitimate interest of the Controller includes, by way of example and not exhaustively:

fraud prevention;

physical and IT security;

defence in court;

evidentiary preservation of data and documentation;

quality control;

prevention of contractual abuse;

internal audits;

exercise of the Controller's rights;

operational continuity and business continuity.

4. Provision of data and consequences of refusal

4.1 The provision of the data necessary for the execution of the contract and for compliance with legal obligations is mandatory: refusal entails the impossibility of concluding the contract or performing the Service.

4.2 The provision of data for promotional purposes and for non-technical cookies is optional. Refusal does not affect the use of the Service.

5. Processing methods and security measures

5.1 Processing takes place with electronic and, where necessary, paper-based tools, with logic correlated to the purposes.

5.2 Smoves adopts adequate technical and organisational measures, in compliance with art. 32 GDPR, to ensure the confidentiality, integrity and availability of the data (access control, authentication, encryption in transit, periodic backups, internal training).

5.3 Access to data is limited to the Controller and to authorised parties, instructed in compliance with art. 29 GDPR.

5.4 Smoves may use automated tools for monitoring, logging, tracking and analysis of accesses and operations performed on company systems, where necessary for security, fraud prevention, technical troubleshooting, audit, judicial protection and continuity of the Service.

5.5 Communications with customer service and with assigned operators may be recorded,

archived and analysed for service quality, internal training, security, complaint management, fraud prevention and protection of the Controller.

6. Storage period

6.1 Personal data are stored for the time necessary to pursue the purposes indicated in this notice and, in any case, within the limits permitted by applicable law. In particular:

contractual, administrative and tax data: up to 10 years from the termination of the relationship;

technical logs, security data, anti-fraud systems and operational records: up to 24 months, except for further storage necessary for security or judicial protection;

photographs, videos, images of packages, seals and operational documentation: up to 24 months from the conclusion of the Service;

documentation relating to complaints, disputes, claims or controversies: up to 10 years from the final closure of the controversy;

data used for marketing purposes: until withdrawal of consent and in any case for a maximum period of 48 months;

data relating to anti-fraud checks, security and abnormal use: up to 10 years in cases of defensive or investigative necessity.

6.2 At the end of the storage period, data are deleted or anonymised, subject to further legal obligations.

6.3 The Controller may store the data for a further period in addition to that indicated above where necessary:

to comply with regulatory obligations;

to exercise or defend a right in court;

upon request of competent Authorities;

in the presence of litigation, investigations or assessments.

7. Recipients and categories of recipients

7.1 The data may be communicated to the following categories of recipients:

Stripe Payments Europe Ltd and Stripe, Inc. for the management of payments, as a processor for the processing activities carried out on behalf of Smoves and as an autonomous controller for its own legal obligations;

IT service providers: website hosting, CRM, booking management tools, transactional emails, appointed as processors pursuant to art. 28 GDPR;

analytics service providers, in anonymised or pseudonymised form (see Cookie Policy);

professional consultants: accountant, labour consultant, lawyer, appointed as processors where the requirements are met, or as autonomous controllers within the limits provided by the Code of Conduct;

parties authorised to hold the storage premises, limited to the data necessary for operational management;

competent Authorities in case of legal obligations.

7.2 The updated list of data processors pursuant to art. 28 GDPR is available upon written request to [Support email].

7.3 Personal data may be communicated to or made available to parent, subsidiary, affiliated companies, commercial partners, consultants, technology providers, parties involved in extraordinary operations or other operators functional to the provision of the Service, within the limits of the purposes indicated in this notice and in compliance with applicable law.

8. Transfers of data outside the EU

8.1 Some providers, in particular Stripe and any analytics and cloud services, may involve the transfer of personal data outside the European Economic Area, also to the United States of America.

8.2 Transfers take place on the basis of one or more of the following instruments provided by Chapter V of the GDPR:

adequacy decision, where applicable, in particular Implementing Decision (EU) 2023/1795 relating to the EU-US Data Privacy Framework;

standard contractual clauses (SCC) adopted by the European Commission;

supplementary measures where necessary in light of the assessment of the third country.

8.3 A copy of the safeguards used may be requested by writing to [Support email].

8.4 The Data Subject acknowledges that some technology providers used by the Controller may carry out processing or sub-processing in non-EU countries. In such cases, the Controller will adopt reasonably suitable measures to ensure a level of protection substantially equivalent to that provided by the GDPR, within the limits of the technical and contractual structure made available by the providers used.

9. Rights of the Data Subject

9.1 The Data Subject, where the legal requirements are met, may exercise the following rights provided by artt. 15-22 GDPR:

access to personal data (art. 15);

rectification of inaccurate or incomplete data (art. 16);

erasure of data ("right to be forgotten"), within the limits of art. 17;

restriction of processing (art. 18);

data portability (art. 20);

objection to processing based on legitimate interest (art. 21);

withdrawal of consent given for optional purposes, without prejudice to the lawfulness of prior processing;

lodging a complaint with the Italian Data Protection Authority (https://www.gpdp.it) or with the Authority of the Member State of residence.

9.2 Requests may be sent, also by ordinary email, to the address [Support email]. Smoves responds within 30 days, except for justified extension of up to 60 additional days.

9.3 Smoves may request information useful to confirm the Data Subject's identity, in compliance with the minimisation principle.

9.4 The exercise of the Data Subject's rights may not entail the deletion or anonymisation of data whose storage is necessary:

for legal obligations;

for evidentiary purposes;

for fraud prevention;

for protection of the Controller in court;

for management of pending disputes;

for system security and operational continuity.

9.5 In the case of manifestly unfounded, excessive, repetitive or disproportionate requests, Smoves reserves the right to:

request a reasonable expense contribution;

refuse the request within the limits permitted by art. 12 GDPR.

10. Automated decision-making and profiling

10.1 Smoves may use automated tools for risk analysis, fraud prevention, anomaly detection, IT security and operational monitoring which, although not normally producing direct legal effects on the Data Subject pursuant to art. 22 GDPR, may contribute to operational assessments relating to the provision of the Service.

11. Data breach

11.1 In the event of a personal data breach, Smoves promptly assesses the incident and, where the requirements are met, notifies the Italian Data Protection Authority within 72 hours of becoming aware of the event, pursuant to art. 33 GDPR, and communicates the breach to the Data Subject without undue delay in the cases provided by art. 34 GDPR.

11.2 Smoves maintains an internal register of breaches and mitigation interventions.

11.3 Smoves cannot be held liable for personal data breaches arising from:

events outside its reasonable control;

wilful or negligent conduct of the Data Subject;

vulnerabilities or unavailability of third-party services;

sophisticated cyber-attacks not preventable with reasonably adequate measures according to the state of the art.

12. Amendments to the notice

12.1 Smoves reserves the right to modify, supplement or update this notice at any time, including as a consequence of:

regulatory changes;

technological developments;

operational variations;

introduction of new services;

organisational or corporate changes.

The amendments will be effective from the date of publication on the website or from the different date possibly indicated.

12.2 Last update date: [Last update date].

13. Specific clauses

13.1 Evidentiary preservation. Smoves may store photographic documentation, operational logs, system recordings, communications and further evidentiary elements for the purpose of protecting its rights, preventing abuse and managing business risk, also beyond the ordinary storage terms, within the limits permitted by applicable law.

13.2 Aggregated and anonymised use of data. Smoves may use aggregated, anonymised or non-directly identifiable data for statistical, research, development, Service optimisation, business analysis and system improvement purposes.

13.3 Anti-fraud checks and operational suspension. Smoves reserves the right to carry out security checks and anti-fraud verifications, including automated ones, and to temporarily suspend the provision of the Service in the presence of:

operational anomalies;

inconsistencies in the data provided;

suspected fraudulent activities;

breaches of the Terms of Service;

risks to the security of the Service or of third parties.