PRIVACY POLICY

Notice on the processing of personal data

pursuant to Articles 12, 13 and 14 of Regulation (EU) 2016/679 ("GDPR")

and of Legislative Decree No. 196 of 30 June 2003 ("Privacy Code"), as amended by Legislative Decree No. 101/2018

Art. 1 – Introduction and regulatory framework

This Privacy Policy is drafted in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data (hereinafter "GDPR"), with Legislative Decree No. 196 of 30 June 2003 ("Privacy Code"), as amended by Legislative Decree No. 101 of 10 August 2018, and with the measures and guidelines of the Italian Data Protection Authority (Garante) and of the European Data Protection Board (EDPB).

This notice describes the manner in which the personal data of data subjects who come into contact with **Hotel Trevi Collection S.r.l.** are processed, including, by way of example and not limitation: website users, customers, suppliers, employees and collaborators, candidates for job positions, visitors to company premises.

The Data Controller undertakes to process personal data in compliance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality set out in Art. 5 GDPR, as well as the principles of data protection by design and by default set out in Art. 25 GDPR.

Art. 2 – Data Controller

The Data Controller is:

Hotel Trevi Collection S.r.l.
TAX CODE / VAT NUMBER: **12065311008**
REGISTERED OFFICE ADDRESS: **VIA GREGORIANA 56 - CAP 00187 - ROMA**
LEGAL REPRESENTATIVE AND DATA CONTROLLER: **PALERMO LINO**
PHONE: **06 69923273**
EMAIL: **info@trevicollectionhotel.com**
PEC (CERTIFIED EMAIL): **hoteltrevicollectionsrl@legalmail.it**

Art. 3 – Data Protection Officer (DPO)

The Data Protection Officer, appointed pursuant to Art. 37 GDPR, may be contacted at the following details: dpo@hideea.com

Hideea S.r.l. - Dr. Antonello Dionisi

Art. 4 – Categories of personal data processed

In carrying out its activity, the Data Controller processes the following categories of personal data:

Identification and contact data

First name, surname, date and place of birth, tax code, address of residence or domicile, e-mail address, landline and mobile telephone number, identity document details.

Browsing and website usage data

IP address, browser type, operating system, date and time of access, pages visited, time spent, any referrer. For cookies and tracking tools, please refer to the specific [Cookie Policy / extended cookie notice].

Data relating to the contractual relationship

Data relating to the performance of the contract, such as bank details and payment data, data relating to orders, invoices, commercial correspondence, data necessary for compliance with tax and accounting obligations.

Data relating to employees and collaborators

Personal data, data relating to the employment relationship (job classification, remuneration, attendance, leave, sickness, accidents, training, appraisals), social security and welfare data, data relating to disciplinary measures, bank details for salary payment, data on dependent family members relevant for tax and social security purposes.

Data relating to suppliers and business partners

Company name, VAT number, data of the legal representative and of business contacts, bank details, contact data, data relating to service quality.

Data collected through video surveillance

Video images recorded by the video surveillance systems installed at the Data Controller's premises, within the limits and in the manner set out in the specific notice posted on the premises.

Special categories of data (pursuant to Art. 9 GDPR)

The Data Controller may process data relating to health, sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership,

as well as genetic and biometric data, only in cases where processing is necessary for the performance of the employment relationship, for compliance with legal obligations, for purposes of preventive or occupational medicine, or subject to the explicit consent of the data subject, and in any case in compliance with the safeguards set out in Art. 9 GDPR and Art. 2-septies of the Privacy Code.

Data relating to criminal convictions and offences (pursuant to Art. 10 GDPR)

The Data Controller may process such data exclusively in the cases and with the safeguards provided for by Art. 10 GDPR and Art. 2-octies of the Privacy Code, in particular for compliance with legal obligations in the field of employment, for verifying good conduct requirements provided for by law, or for the establishment, exercise or defence of a right in judicial proceedings.

Art. 5 – Purposes of processing and legal bases

The following table summarizes, for each category of data subjects and processing activity, the purposes pursued and the corresponding legal basis pursuant to Art. 6 GDPR, as well as, where applicable, the conditions of lawfulness for special categories of data pursuant to Art. 9 GDPR and for data relating to criminal convictions pursuant to Art. 10 GDPR.

Data subjects	Processing activity	Purpose	Legal basis (Art. 6)	Conditions for data under Arts. 9-10
Customers / Users	Management of the contractual and pre-contractual relationship	Performance of the contract, preparation of quotes, order management, invoicing, after-sales support	Art. 6.1.b – Performance of a contract or of pre-contractual measures	—
Customers / Users	Compliance with tax, accounting and administrative obligations	Keeping of accounting records, issuance of invoices, tax returns, document retention	Art. 6.1.c – Legal obligation	—
Customers / Users	Direct marketing activities	Sending of commercial communications, newsletters, promotions relating to products/services similar to those already purchased	Art. 6.1.a – Consent (new customers) / Art. 6.1.f – Legitimate interest (existing customers, soft spam pursuant to Art. 130, para. 4, Privacy Code)	—
Customers / Users	Commercial profiling activities	Analysis of preferences, consumption habits and choices for	Art. 6.1.a – Consent (revocable at any time)	Art. 9.2.a – Explicit consent (if special

Data subjects	Processing activity	Purpose	Legal basis (Art. 6)	Conditions for data under Arts. 9-10
		sending personalized offers		categories are involved)
Employees / Collaborators	Management of the employment relationship	Establishment, performance and termination of the relationship, management of attendance, remuneration, leave, sickness, training, appraisals	Art. 6.1.b – Performance of the employment contract; Art. 6.1.c – Legal obligation (labour law regulations)	Art. 9.2.b – Obligations and rights in the field of labour law; Art. 9.2.h – Preventive and occupational medicine
Employees / Collaborators	Social security, welfare and tax obligations	Payment of contributions, adjustments, returns, mandatory communications to the competent bodies	Art. 6.1.c – Legal obligation	Art. 9.2.b – Obligations in the field of social security
Employees / Collaborators	Management of disputes and disciplinary proceedings	Establishment, exercise or defence of a right in judicial or extrajudicial proceedings; management of disciplinary proceedings	Art. 6.1.f – Legitimate interest; Art. 6.1.c – Legal obligation (Art. 7 of the Workers' Statute)	Art. 9.2.f – Establishment, exercise or defence of a right
Suppliers / Partners	Management of the supply relationship	Selection, contracting, order management, payments, quality assessment	Art. 6.1.b – Performance of the contract	—
Suppliers / Partners	Tax and accounting obligations	Keeping of accounting records, invoice registration, tax returns	Art. 6.1.c – Legal obligation	—
Visitors / Website users	Website browsing	Enabling browsing, ensuring website security, anonymous statistics	Art. 6.1.b – Performance of the browsing service; Art. 6.1.f – Legitimate interest (security); Art. 6.1.c – Legal obligation (investigation of computer crimes)	—

Data subjects	Processing activity	Purpose	Legal basis (Art. 6)	Conditions for data under Arts. 9-10
Visitors / Website users	Cookies and tracking tools	Technical cookies: website operation. Analytics cookies: aggregate statistics. Profiling cookies: personalized marketing	Art. 6.1.a – Consent (for non-technical cookies); Art. 122, para. 1, Privacy Code – exemption for technical cookies	—
Visitors to company premises	Video surveillance	Protection of the safety of persons and property, prevention of unauthorized access and unlawful acts	Art. 6.1.f – Legitimate interest (security); Arts. 4 and 114 Privacy Code; Garante Order of 8 April 2010	—

Art. 6 – Manner of processing and security measures

6.1 General procedures

The processing of personal data is carried out by manual, computerized and telematic means, with logic strictly related to the purposes indicated and, in any case, in such a way as to guarantee the security and confidentiality of the data, in compliance with Art. 32 GDPR.

6.2 Technical and organizational security measures

The Data Controller has adopted adequate technical and organizational measures to ensure a level of security commensurate with the risk, including:

- control of physical access to premises and to IT systems;
- authentication and profiling of users with personal credentials and complex password policies;
- logging of access to systems and databases;
- firewalls, intrusion detection systems, antivirus software and periodic system updates;
- periodic backups and disaster recovery procedures;
- encryption of communications and, where necessary, of archived data;
- periodic training of personnel authorized to process data;
- procedures for managing personal data breaches pursuant to Arts. 33 and 34 GDPR;
- data protection impact assessment (DPIA) pursuant to Art. 35 GDPR, where required.

6.3 Principle of minimization

Pursuant to Art. 5, para. 1, letter c), GDPR, data is processed to the extent that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The Data Controller periodically verifies the relevance and non-excessiveness of the data collected, deleting any data that is not necessary.

6.4 Persons authorized to process data

Pursuant to Art. 29 GDPR and Art. 2-quaterdecies of the Privacy Code, personal data is processed exclusively by natural persons authorized to process data who operate under the direct authority of the Data Controller or of the Data Processor, on the basis of specific instructions given in writing and following adequate training.

Art. 7 – Recipients and categories of recipients of personal data

Personal data may be disclosed to the following categories of recipients:

Persons internal to the Data Controller

Employees and collaborators of the Data Controller expressly authorized to process data, each within the limits of their duties and in accordance with the need-to-know principle.

Data Processors (pursuant to Art. 28 GDPR)

Third parties appointed as Data Processors by means of a specific contract or legal instrument, who carry out technical and organizational services on behalf of the Data Controller, including, by way of example:

- providers of IT and hosting services;
- providers of website management and maintenance services;
- providers of e-mail and communication services;
- tax, accounting, legal and labour law consultants;
- providers of payroll and personnel management services;
- providers of video surveillance and security services;
- banking and insurance institutions;

The updated list of Data Processors is available at the Data Controller's premises and may be requested at the contact details set out in Art. 2.

Independent Data Controllers

Persons who process data as independent Data Controllers, such as:

- social security and welfare bodies (INPS, INAIL);
- the Italian Revenue Agency and other public bodies;
- judicial authorities and police bodies;
- administrative supervisory authorities (Data Protection Authority, Labour Inspectorate, etc.);
- providers of statistical analysis and/or profiling services (as independent Data Controllers, whose notices are available on their respective websites).

Disclosure to third parties for legal obligation

Data may be disclosed to third parties when disclosure is required by a legal provision or by an order of the judicial authority.

Dissemination

Personal data is not disseminated, except where there is a legal obligation or the explicit consent of the data subject.

Art. 8 – Transfer of personal data to third countries or international organizations

General rule

The Data Controller processes personal data predominantly on servers located within the territory of the European Union.

Transfers to third countries

Where, for the performance of certain processing operations (e.g. cloud services, analytics, communications), personal data is transferred to third countries outside the European Economic Area, the transfer takes place:

- on the basis of an adequacy decision of the European Commission pursuant to Art. 45 GDPR;
- or on the basis of Standard Contractual Clauses adopted by the European Commission pursuant to Art. 46, para. 2, letter c), GDPR, supplemented, where necessary, by additional technical and organizational measures;
- or, in the absence of the above conditions, on the basis of the derogations provided for by Art. 49 GDPR (explicit consent of the data subject, performance of a contract, etc.).

The data subject may obtain a copy of the safeguards adopted for the transfer by contacting the Data Controller at the contact details set out in Art. 2.

Art. 9 – Data retention periods

Personal data is retained for a period not exceeding that necessary to achieve the purposes for which it was collected, in accordance with the storage limitation principle set out in Art. 5, para. 1, letter e), GDPR. The criteria used to determine the retention period are set out in the following table:

Data category	Retention period	Criterion / Regulatory reference
Data relating to customers (contractual and accounting)	10 years from termination of the	Art. 2220 Civil Code (retention of accounting records); Art. 22

Data category	Retention period	Criterion / Regulatory reference
	relationship or from the last transaction	Presidential Decree 600/1973 (tax obligations)
Data for marketing purposes	24 months from the last contact or until withdrawal of consent	Principle of minimization and Garante orders
Data for profiling purposes	12 months from collection, unless consent is renewed	Garante cookie guidelines and Garante orders
Data relating to employees	10 years from termination of the relationship (remuneration and contribution data); 5 years for other data	Art. 43 Presidential Decree 600/1973; five-year limitation period for employee rights (Art. 2948 Civil Code)
Data relating to job applicants	24 months from collection of the CV, unless consent is given for further retention	Garante orders and principle of minimization
Browsing data (logs)	7-30 days, unless required for the investigation of crimes	Garante orders and principle of minimization
Video surveillance data	24-48 hours, unless required for investigation purposes or in the case of holidays/extended closures (max. 7 days)	Garante Order of 8 April 2010
Data relating to suppliers	10 years from termination of the relationship	Art. 2220 Civil Code and tax obligations

Upon expiry of the retention periods, data is deleted or irreversibly anonymized, unless further retention is necessary to comply with a legal obligation, to establish, exercise or defend a right in judicial proceedings, or for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes (Art. 89 GDPR).

Art. 10 – Nature of the provision of data and consequences of refusal

The provision of personal data is:

- **mandatory** when necessary for the performance of the contract, for compliance with a legal obligation or for the performance of a task carried out in the public

interest. In such cases, refusal to provide the data makes it impossible to establish or continue the relationship;
- **optional** when based on consent or on legitimate interest. In such cases, refusal has no consequences on the main relationship, but precludes the carrying out of the activity for which the data is requested (e.g. marketing, profiling).

For each processing activity, the mandatory or optional nature of the provision of data is specified in the detailed notice given to the data subject at the time of collection.

Art. 11 – Rights of the data subject

11.1 List of rights

Pursuant to Arts. 15-22 of the GDPR, the data subject has the right to exercise the following rights against the Data Controller at any time:

Right	Regulatory reference	Content
Access	Art. 15 GDPR	Obtain confirmation of the existence of processing and access to one's own personal data and to the information referred to in this notice
Rectification	Art. 16 GDPR	Obtain the correction of inaccurate personal data or the completion of incomplete data
Erasure (right to be forgotten)	Art. 17 GDPR	Obtain the erasure of personal data, in the cases provided for by law
Restriction of processing	Art. 18 GDPR	Obtain the restriction of processing where the conditions set out by law are met
Portability	Art. 20 GDPR	Receive data in a structured, commonly used and machine-readable format, and transmit it to another Data Controller, where technically feasible
Objection	Art. 21 GDPR	Object to processing for reasons connected with one's particular situation, including processing for direct marketing purposes
Withdrawal of consent	Art. 7, para. 3, GDPR	Withdraw consent at any time, without affecting the lawfulness of processing based on consent given before its withdrawal

Right	Regulatory reference	Content
Complaint	Art. 77 GDPR	Lodge a complaint with the Data Protection Authority (Garante) (www.gpdp.it) or seek judicial remedy (Art. 79 GDPR)

11.2 Manner of exercising rights

The exercise of rights is free of charge pursuant to Art. 12, para. 5, GDPR. To exercise their rights, the data subject may send a written request to the Data Controller at the contact details indicated in Art. 2. The Data Controller shall respond without undue delay and, in any case, within one month of receipt of the request, a period that may be extended by a further two months where necessary, taking into account the complexity and number of requests. The Data Controller shall inform the data subject of any such extension and of the reasons for the delay within one month of receipt of the request.

11.3 Limitations on the exercise of rights

The rights referred to in Arts. 15-22 GDPR may be limited in the cases provided for by Arts. 2-undecies and 2-duodecies of the Privacy Code (e.g. activities of parliamentary boards of inquiry, defensive investigations, exercise of a right in judicial proceedings, safeguarding of interests protected in relation to money laundering).

Art. 12 – Automated decision-making and profiling

12.1 Automated decisions

The Data Controller does not adopt decision-making processes that are entirely automated and that produce legal effects significantly affecting the data subject or that similarly significantly affect the data subject, pursuant to Art. 22 GDPR, without prejudice to what may be specified in detailed notices for individual processing operations.

12.2 Profiling

Where the Data Controller carries out profiling activities (e.g. analysis of consumption preferences for personalized marketing purposes), such processing is subject to the explicit consent of the data subject and is described in the specific notice given at the time consent is collected.

Art. 13 – Personal data breach

The Data Controller has adopted procedures to detect, manage and notify personal data breaches. In the event of a breach presenting a risk to the rights and freedoms of data subjects, the Data Controller notifies the breach to the Garante within 72 hours of becoming aware of it, pursuant to Art. 33 GDPR. Where the breach presents a high risk to the rights and freedoms of data subjects, the Data Controller also communicates the breach to the data subjects without undue delay, pursuant to Art. 34 GDPR.

Art. 14 – Amendments and updates

This Privacy Policy is subject to periodic revision. Any changes will be published on the Data Controller's website in the dedicated section and, where significant, will be communicated to data subjects through the available contact channels (e-mail, website notices, specific notices). Data subjects are invited to periodically consult this notice to check for any updates.

The date of the last update is shown at the foot of this document.

Art. 15 – Reference to specific notices

This Privacy Policy contains general information on the processing of personal data carried out by the Data Controller. For specific processing activities (cookies, video surveillance, personnel selection, etc.), the Data Controller makes detailed notices available through:

- the institutional website, in the [Privacy / Cookie Policy] section;
- the physical premises (for the video surveillance notice);
- the specific communications given at the time of data collection.

The specific notices supplement and detail this Privacy Policy, together forming a layered information system, in accordance with the EDPB Guidelines on transparency (formerly WP29).

6 July 2026