SARDINERO HOTELES

Integrated Website Privacy Policy | English translation of Spanish edition 02 dated 22 January 2021

This document translates the supplied Spanish privacy policy. It describes the processing carried out by EL SARDINERO, S.A. (Sardinero Hoteles) as stated in that policy.

Privacy policy and your rights

The policy states that EL SARDINERO, S.A. complies with Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR) and Spanish Organic Law 3/2018 on Personal Data Protection and the Guarantee of Digital Rights (LOPDGDD), and applies security measures intended to protect the confidentiality of personal data.

Data controller

EL SARDINERO, S.A. (SARDINERO HOTELES) | C/Cádiz, 22, 39002 Santander (Cantabria), Spain | Telephone: 942 205 000 | Email: gdpr@sardinerohoteles.com

Your rights

- You may obtain confirmation as to whether personal data concerning you are being processed.
- You may access your personal data and request rectification of inaccurate data or, where applicable, erasure when the data are no longer necessary for the purposes for which they were collected.
- The policy says rectification is not possible for CCTV footage because the images record objective events in reality.
- In certain circumstances, you may request restriction of processing; restricted data will be retained only for the establishment, exercise or defence of claims.
- In certain circumstances, you may object to processing on grounds relating to your particular situation. The controller will stop processing unless there are compelling legitimate grounds or the data are needed for claims. The policy notes that an objection to CCTV processing may not be capable of being upheld where security interests prevail.
- You may receive personal data concerning you in a commonly used, structured, machine-readable format and transmit them to another controller, where the right to data portability applies.
- Where processing is based on consent, you may withdraw consent at any time; withdrawal does not affect the lawfulness of processing carried out before withdrawal.

How to exercise your rights

Send your request to gdpr@sardinerohoteles.com. The policy asks you to provide a written description of the request; proof of identity (name, surname and a copy of the requester’s national identity document, and, where applicable, the representative’s document and proof of representation); a postal address for notices and a date and signature for a letter, or your full name for an email. Requests may also be validated through a private communication channel using a personal identity-authentication key.

For requests concerning data of a deceased person, the policy lists documents that may be requested: a family record book or civil registry certificate showing the relationship; a will naming the requester as heir; an express designation by the deceased; or proof of legal representation. For requests to rectify or erase a deceased person’s data, it also requests a declaration that the other family members or persons linked by a relationship and the heirs agree. The controller may request further information if it has reasonable doubts about identity.

A rectification request should identify the data and the correction sought and include supporting documents where needed. If a large quantity of data is processed, the controller may ask you to specify which data or processing activities your access request concerns.

Handling and response times

- The controller will provide information about action taken on requests under GDPR Articles 15–22 within one month. This period may be extended by up to two further months where necessary because of complexity or the number of requests; you will be told within the first month and given the reasons.

- Where a request is made electronically, the response will be provided electronically where possible, unless you ask otherwise. Where available, secure remote access may satisfy an access request, without limiting your right to request information under GDPR Article 15(1) that is not included in that system.
- If the controller does not act on your request, it will explain why within one month and inform you of your right to complain to a supervisory authority and seek a judicial remedy.
- Information is free of charge, except for a reasonable fee for administrative costs. A disproportionate alternative delivery method may result in you bearing the additional cost. The controller may refuse manifestly unfounded or excessive requests and must be able to demonstrate that basis; repeated access requests more than once in six months may be treated as repetitive unless there is legitimate cause.
- Where rectification or erasure applies, data may be blocked: identified and stored with technical and organisational safeguards preventing processing, except for making them available to courts, the Public Prosecutor's Office or competent public authorities for the establishment of liabilities, and only for the applicable limitation period; they are then destroyed.
- Where erasure follows an objection to direct marketing, identifying data may be retained to prevent future direct-marketing processing. The policy refers users to advertising opt-out systems published by the Spanish Data Protection Agency (AEPD) at www.aepd.es.
- For CCTV, footage is generally retained for one month. To protect third-party rights, access may be answered by a certificate describing the processing rather than direct access to footage showing other people.

If you consider that your rights have not been properly addressed, you may complain to the competent data-protection authority. The policy refers to www.agpd.es and, in its final CCTV section, to the Spanish Data Protection Agency, C/ Jorge Juan, 6, 28001 Madrid.

Additional information for contact data

Purposes

- Answering enquiries, complaints, incidents and requests for technical, corporate or activity information, and handling related communications and service coordination.
- Registering people for Sardinero events and managing newsletter subscriptions.
- Sending satisfaction surveys, news, corporate information, offers and promotions, where consent has been given.
- Taking and publishing audiovisual or graphic material in corporate or public media for reporting, promotion, campaigns, activities and events, where consent has been given.
- Handling corporate restructuring or business transfers where necessary to complete the transaction and, where applicable, maintain services.
- Recording reports of conduct that may breach applicable rules in the organisation's reporting channel, including anonymous reports.

Retention, legal basis and recipients

Contact data are retained while the lawful relationship continues and, after it ends, unless erasure is requested, subject to retention needed for claims, another person's rights or a legal obligation. Marketing data are kept until consent is withdrawn. Reporting-channel data are retained to decide whether to investigate and later as evidence of the organisation's crime-prevention model.

The policy identifies performance of the request, the controller's legitimate interests and the person's consent as legal bases. Legitimate interests include defending the controller's interests, compliance, and the specific processing activities set out in the LOPDGDD. Data may be shared with service providers and collaborators, the compliance unit or designated processors, law-enforcement bodies where justified, and media or specialist publications for promotion. Third-party recipients must have a personal-data protection system consistent with applicable law.

Data are obtained from the person concerned, including through communications or professional social networks. Categories include identity and contact details, information supplied in enquiries or requests, complaints and incidents, and personal data about third parties supplied by the person. Access is restricted to authorised Sardinero Hoteles personnel, processors and hotel/activity personnel; confidentiality commitments and IT security measures are used.

Additional information for customer data

Purposes

- Internal administration, accounting and operations arising from accommodation, restaurant and event services; offering, contracting and providing services and meeting contractual requirements.
- Responding to enquiries, complaints, incidents, information requests and activity requests; managing contacts and visits.
- Promoting the organisation through statistics, activity reports, case studies, campaigns, events and audiovisual material; sending newsletters and corporate information.
- Assessing service quality and stakeholder satisfaction; supplying evidence of technical capability for bids, projects, events and grants.
- Compliance monitoring and audits, including access controls and use of CCTV images to investigate incidents, workplace-rule breaches, offences or unlawful conduct.
- Profiling to offer products and services suited to customer interests and improve user experience; the policy says no automated decisions will be made on the basis of the profile.
- Creditworthiness assessment, statistical and historical purposes, environmental and workplace-safety management, direct-marketing offers and Christmas greetings, and consultation of advertising-exclusion systems.
- Handling corporate restructuring or business transfers; recording reports of potentially unlawful conduct. The policy also reserves periodic audits at customer and debtor premises under deposit contracts and describes international transfers where strictly necessary for a project outside the EU.

Retention

Customer data are retained while the lawful relationship continues, subject to legal retention, claims and protection of others' rights. At the end of the relationship, data are blocked as required by applicable data-protection rules. The policy gives these examples: hotel guest registration records, three years; tax records, generally four years (with a ten-year limitation period for certain offences); commercial books and supporting documents, six years; CCTV footage, 30 days except where preservation is legally required; building-access records, 30 days; creditworthiness-file data while the breach persists, up to five years from the debt due date; marketing data until consent is withdrawn; and data needed for legal or contractual claims, including the stated five-year civil-liability period. Data related to legal guarantees are retained for the guarantee period and any subsequent claim period. Reporting-channel data are retained to determine whether an investigation is warranted and as evidence of the crime-prevention model.

Legal basis and recipients

The policy identifies contract performance (accommodation, restaurant and event bookings/orders/contracts), compliance with legal obligations, legitimate interests and consent as legal bases. Stated legitimate interests include managing a commercial relationship, internal administration within a group, fraud prevention, protecting assets through CCTV, direct marketing to existing customers for similar products or services, and defending the controller's interests. Consent may be given through the applicable forms or contact channel.

Recipients may include travel agencies and intermediaries, community managers, subcontractors, auditors, financial institutions for payment collection, tax authorities, law-enforcement bodies where legally required, booking or payment processors where the person has consented, media or specialist publications where publication consent has been given, and the compliance reporting channel. The policy also describes international transfers where strictly necessary for a project outside the EU or because processing applications are hosted abroad. Recipients must have a data-protection system consistent with applicable law.

Data may come from the customer, other Sardinero Hoteles companies, travel agencies and intermediaries, or a booking/payment entity with which the controller has a contractual or service relationship. Categories include business and contact details, job-role information, financial and payment details, services received and transactions, representatives' names and tax identification numbers, and contact details of people involved in the service. The policy says specially protected data or criminal-conviction data are not ordinarily included, except information the customer provides to adapt a requested service, such as reduced mobility or food intolerances.

The policy describes access restrictions, confidentiality obligations, contractual safeguards and IT security measures. Where a contracted service could expose Sardinero Hoteles staff to the customer's premises or data, staff are not permitted to access confidential or personal data unless the service scope includes handling such

data. In that case, a data-processing agreement is to specify the subject matter, duration, nature, purpose, data categories, security measures, and the parties' obligations and rights. If the customer does not contract for personal-data processing, Sardinero Hoteles states it does not assume processor responsibility. Any confidential information encountered is subject to an indefinite duty of secrecy.

Additional information for supplier data

Purposes

- Internal commercial, relationship, operational, administrative, accounting and financial management of the supplier/partner relationship.
- Contracting and delivery of services; responding to enquiries, complaints, incidents and requests.
- Promoting and reporting on the organisation, including statistics, activity reports, campaigns, events and publications; sending news and activity updates.
- Quality evaluation; selecting, approving and contracting suppliers/partners and verifying compliance.
- Workplace health and safety, prevention of occupational risks, attendance/timekeeping and performance monitoring.
- Demonstrating technical capability for bids, projects, events and grants; compliance investigations and audits, including access and CCTV controls.
- Contact management, statistical, historical or scientific purposes, access control and site security, environmental and workplace-safety management, corporate restructuring or business transfers, and reporting-channel processing.
- The policy says Sardinero Hoteles reserves the right to conduct periodic audits at suppliers' and creditors' premises.

Retention

Supplier data are retained while the lawful commercial relationship continues, subject to legal obligations and claims. At the end of the relationship, data are blocked. The policy lists examples: tax records, generally four years (with a ten-year limitation period for certain offences); commercial records, six years; occupational-risk-prevention records, five years; CCTV and automated building-access records, 30 days subject to stated exceptions; legal-guarantee data for the guarantee and claim period; creditworthiness data while a default persists, up to five years; and marketing data until consent is withdrawn. Reporting-channel and claims data are retained for investigation, evidence and applicable legal or contractual periods, including the stated five-year civil-liability period.

Legal basis, recipients and data categories

The stated bases are contract performance, legal obligations (including administrative, commercial, tax, accounting, financial, occupational-safety and sector rules), legitimate interests and consent. Recipients may include Sardinero Hoteles hotels, legal advisers, management/compliance auditors, occupational-risk-prevention services, subcontractors, public authorities such as the tax agency, financial institutions, worker representatives where required, and the compliance reporting channel. The policy describes restrictions on access to medical information: under the cited occupational-risk rules, the employer and other third parties may not access medical information, except for conclusions about fitness for work.

Data may come from the person or their legal representative, Sardinero Hoteles hotels, or a contracting/service entity. Categories include company and contact details, information about workers assigned to contracted work, CVs and professional details used to show technical capability, licences and approvals, commercial and financial/payment data, supplied services and transactions, and representative/contact details. The policy says criminal-conviction and sensitive data are not ordinarily included, except where special conditions require supporting information.

Confidentiality and third-party information

A supplier or partner who provides personal data about its contacts, legal representatives, project staff, CVs or subcontracted workers must inform those people, on Sardinero Hoteles' behalf and within one month of disclosure, that their data are communicated to EL SARDINERO, S.A. (gdpr@sardinerohoteles.com). The stated purposes include contractual, employment, occupational-safety and social-security compliance, verification of supplier personnel and maintaining commercial-history records. The policy says the processing is required by law and refusal to provide the data may lead to termination of the contract. Data may be disclosed to authorities and third parties where legally required. Individuals may exercise their rights under the privacy policy and complain to the Spanish Data Protection Agency at C/ Jorge Juan, 6, 28001 Madrid. Suppliers must also maintain confidentiality about information and personal data encountered through their relationship with Sardinero Hoteles, including after that relationship ends.

Additional information for CCTV and access records

Purposes and retention

- Managing access and visits and operating CCTV to protect people, property and premises, support security and compliance, investigate incidents or accidents, manage related insurance, and address breaches of safety rules.
- Checking employees' performance of work duties under Article 20.3 of the Spanish Workers' Statute, and investigating workplace incidents, offences or unlawful conduct.
- Managing occupational health and safety, attendance and time records, and compliance monitoring.
- Temporarily checking body temperature to identify possible infections, prevent access and contact with others, protect health and life, help contain a pandemic, meet occupational-safety obligations and verify that workers attend without fever.
- Recording reports of potentially unlawful conduct through the organisation's reporting channel.

CCTV images and sound are normally deleted within one month (30 days). Where needed to evidence acts affecting people, property or premises, images are made available to the competent authority within 72 hours of becoming aware of the recording. Exceptions also apply to serious or very serious public-security offences, an ongoing police investigation, or open judicial or administrative proceedings. Building-access records are generally retained for 30 days. Temperature-control data are retained for the period considered necessary to address potential legal actions arising from a refusal of access.

Legal basis, disclosures and data categories

The policy cites legitimate interests in security, protection of assets, compliance, investigation of incidents and employment oversight, as well as legal obligations concerning occupational health and safety and the cited COVID-19 protocols. CCTV or access data may be disclosed to contracted security providers, insurers in connection with an incident, law-enforcement authorities, the premises owner where justified by protection of its assets, courts and tribunals, and the compliance channel. Where a temperature reading exceeds the health threshold, access may be refused and the person referred to primary care (external visitors) or occupational health services (internal personnel), in accordance with the protocol.

The data categories listed are images, identifying and professional details, the reason for a visit and the person being visited, and entry and exit times. Temperature data may also be processed during temporary checks under an applicable COVID data-processing protocol. The policy describes the reporting channel as accessible only to internal-control/compliance personnel and designated processors, except where access or disclosure is necessary for disciplinary measures or legal proceedings.

Security measures

- Visible notices identify CCTV processing, the controller and the possibility of exercising GDPR rights; the full information is available in this policy, which may be accessed through a code or web address on the notice.
- Public-road images are captured only to the extent essential for security. Sardinero Hoteles says it does not install CCTV or sound-recording systems in employee rest or leisure areas such as changing rooms, toilets or dining rooms.
- Sound is recorded only where relevant security risks justify it, and subject to proportionality, minimum intervention and safeguards.

- Monitors are kept in restricted-access areas. Access to footage is handled using a recent photograph, identity document and the relevant date and time. Direct access to images showing third parties is not provided; a certificate describing the processing may be issued instead.
- Access to personal data is limited to authorised staff and service providers, who are subject to confidentiality commitments. The policy states that IT security measures and contractual arrangements are used to prevent unauthorised access and protect data.

Changes to this privacy policy and declarations

Sardinero Hoteles reserves the right to modify, vary, remove or cancel the contents or presentation of this policy. It recommends checking the policy periodically. If you disagree with a change, you may exercise your rights using the stated procedure by emailing gdpr@sardinerohoteles.com.

The policy states that information supplied, including personal data about other people, is processed for the purposes described in the policy. The person providing it declares that they have been informed and consent, and that they have informed third parties and obtained any consent required for their data to be processed.

By entering premises subject to CCTV, a person is stated to expressly consent to the processing described in the privacy clause and additional information, and to inform third parties whose personal data they provide for access registration. By accepting or validating the process, the person declares that they are over 14 and legally capable and expressly consents to the processing described. Where consent boxes are selected, consent is the legal basis and may be withdrawn at any time. A person representing a child under 14 or a person lacking legal capacity declares that they hold parental responsibility, guardianship or the relevant legal authority; the controller may request evidence.