IS-POL-01

VERSION 2.0

08/01/2024

DOCUMENT CLASSIFICATION: INTERNAL USE

INFORMATION SECURITY POLICY

Contents

ABBREVIATIONS / TERMS USED

The following abbreviations and terms are used within all documents of the Compliance Manual:

Assets	Assets related to information and its life-cycle
Company:	Fattal Hotel Management (Cyprus) ltd
DPA	Data Protection Agreement
DPIA	Data Protection Impact Assessment
DPO:	Data Protection Officer
GDPR - ISMS:	Information Security Management System that complies with the GDPR
H/W:	Hardware
ICT:	Information and Communication Technology
IT Administrator:	The Administrator of an ICT System
NDA:	Non-disclosure agreement

1. SCOPE OF THE POLICY

The purpose of this document is to present a summary of the decisions, practices and processes adopted by the company that are related to the Management of Information Security and the protection of Personal Data. Through this specific document the company presents as a summary the general principles, objectives and guidelines in relation to the security of corporate information and the protection of personal data which it processes. This policy is an integral part of the entire System that is consisting by several specific Policies, Procedures and documents supporting the Policies and Procedures, and proving their implementation.

Under the provisions of this Policy and the Compliance System, must fully commit the managers and the employees (irrespective of position and whether they are permanently or part-time employed or they are under any type of contracts, or if they are under a training or probation period).

The following natural and legal persons shall also be bound to this Policy and the specific GDPR-ISMS provisions that are properly communicated to them:

- All the staff members of legal entities-external partners, in case they have access to and are processing of corporate non-public information and for the entire duration this legal person performs these duties and even after that period;
- External partners – natural persons under the same condition of processing corporate non-public information;
- Any subcontractors acting as company's processors.

In case the above natural or legal persons are contracting with subcontractors, these subcontractors shall also have to be bound to this policy and the specific GDPR-ISMS provisions that the main contractor is bound to follow.

The Company undertakes to disclose this Policy to any existing or new employee, affiliate, trainee, processor, and to ensure by all appropriate means, their knowledge and commitment, for the proper compliance to the Policies and the practices described therein for processing non-public information.

The GDPR-ISMS of the company cover Primary and Supportive assets, and thus, it includes:

- Employees;
- Premises;
- Information systems and applications that support corporate processes;
- Software applications and tools that are used;
- Software that supports corporate processes and is provided by service provider (i.e., internet, email);
- Central system's hardware and software;
- Workstations, portable devices and related software;
- Peripheral equipment;
- Cable infrastructure, active and passive network equipment, wireless networks, other telecommunication equipment to the relevant extent;

- Information (in electronic or physical form) as a Primary asset.

The Company, through the implementation of the GDPR-ISMS:

- ✓ Complies with the legal framework regarding the processing of Personal Data of Natural Persons and ensures such compliance;
- ✓ Follows the main provisions of the ISO 27001 Standard that are related to the processing of Personal Data and the security of corporate information and in accordance to the supervising Personal Data Protection Authority's announced guidelines;
- ✓ Defines the input and the expected results of its processes;
- ✓ Specifies the interaction between its processes;
- ✓ Specifies the criteria and methods of monitoring;
- ✓ Specifies the required resources;
- ✓ Assigns roles and responsibilities;
- ✓ Encounters the risks/ threats and take advantage of the opportunities;
- ✓ Implements improvement actions.

1.1. Structure of the GDPR-ISMS

The GDPR-ISMS consists of:

- The present summary, which includes the objectives of the company for the protection of its information and the personal data, the commitment of its Management to implement the system and continuously improve it, as well as the basic provisions of the information security and personal data protection in short (summary).
- A set of individual specific Policies, designed to define detailed information in various areas regarding information security and the protection of personal data, the way these Policies are implemented, defined within the policies or in specific Procedures and the documentation proving Company's compliance (forms, templates, work instructions etc.).

2. APPLICATION FIELD & DISTRIBUTION

This policy is horizontal and applies in Group and Hotel level and is distributed to the head of the departments / organisational units, so as to inform staff members of their unit. It shall also be available to all interested parties giving them the opportunity to be properly informed on decisions and processes.

3. DEFINITIONS

- HGM: Hotel General Manager
- RGM: Regional General Manager
- DPO: Data Protection Officer
- GQHSM: Group Quality, Health & Safety Manager
- IMS: Integrated Management System

- GDPR: General Data Protection Regulation

4. BASIC GDPR-ISMS TERMINOLOGY

Personal Data means any information relating to an identified or identifiable natural person (‘**data subject**’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as (indicatively) a name, an identification number, age, permanent address and contact details, occupation, bank details, education, work, an identifier related to information and communication technologies such as Internet Protocol address etc., or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on information and/or personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third party means a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Confidentiality means a characteristic of the information by which it is available only to authorised persons or systems.

Integrity means a characteristic of the information by which it is changed only by authorised persons or systems in an allowed way.

Availability means a characteristic of the information by which it can be accessed by authorised persons when it is needed.

Business Continuity means the advance planning and preparation undertaken to ensure that the company will have the capability to operate its critical business functions during emergency events with the minimum interruption.

Information security is including preservation of confidentiality, integrity and availability of information as major principles.

GDPR - ISMS is part of the overall management processes which takes care of planning, implementing, maintaining, reviewing, and improving the information security and the protection of personal data and the privacy of natural persons.

5. MAIN OBJECTIVES OF LEONARDO GDPR-ISMS

Through the GDPR-ISMS, the company aims to ensure the main principles of Confidentiality, Integrity and Availability. All parties that are bound to this policy have to ensure:

Confidentiality: Ensuring that access to information is available only to those who are duly authorised;

Integrity: Ensuring that information is complete, accurate, and valid;

Availability: Ensuring that the information is available whenever an authorised user attempts to access it.

In addition to the above three key security objectives, the Company aims to ensure:

User identification and authentication: Ensuring that the user attempting to access information / system / application is the one it claims to be.

Access Control: Ensuring that the user attempting to access information / system / application is authorised for this action.

Audit and Monitoring: Ensuring that users' actions are properly recorded and monitored.

Disclaimer prevention: Ensuring that a user cannot refuse that he/she has performed an action related to accessing or processing of information / system / application.

The company, through its Compliance System, achieves and ensures all of the above security objectives, resulting in the highest possible protection of personal data, information, systems and applications.

The GDPR-ISMS System is also aiming:

- To provide management direction and support for information security and personal data protection in accordance with business and contractual requirements and the relevant laws and regulations;
- To prevent waste or inappropriate use of corporate ICT resources;
- To minimise till nullification of incidents related to the confidentiality, integrity and availability of information and personal data;
- To reduce failures and improve work efficiency and effectiveness; reduce complaints and increase customer and stakeholder satisfaction through the provision of quality and secure services;
- To protect company's reputation, create a better market image and provide guidelines for the protection and the use of information technology assets and resources within the business, so as to ensure confidentiality, integrity and availability of data and assets;

- To minimise time of disruption in case of incidents that endanger the continuous provision of services;
- To apply a standard in the company regarding Information Security and Ethics on usage of Technology.

The company with regards to its information security follows the process of

5.1. Organisational Structure and Roles

The company has defined its organisational structure and has specified the roles that are responsible or related to the management of its information security. Through these specific structure and roles, the company aims to protect its information and the related resources against unauthorised access, disclosure, alteration or destruction.

The organisation of the information security has properly been disclosed to the staff and need to know third parties and includes the following roles:

- Top Management holding the overall responsibility to manage the system, practically expressed through a variety of roles;
- Data Protection Officer supports the Company, employees and related 3rd parties regarding issues coming from the GDPR Regulation;
- IT Administrator manages day-to-day operations of the assigned ICT systems, and controls and administers systems and users;
- Users are the staff members using devices, systems and information resources to carry out their daily duties.

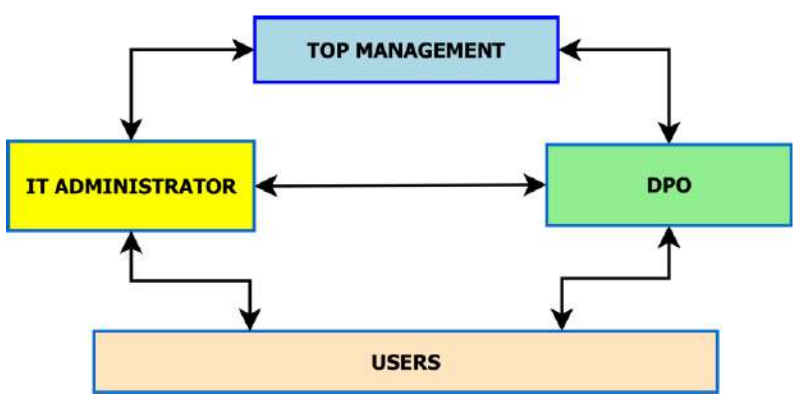

Figure 1: Roles and interactions regarding the GDPR in Fattal Hotel Management (Cyprus) Ltd

The Company has taken the proper organisational measures in order to achieve a clear separation of duties and responsibilities between the different roles. In particular, a user's access to company information resources may be authorised, with appropriate authorisation from another role, in an upper scale of the hierarchy. The separation of duties serves two aims:

The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls.

5.2. Management of Information Resources and Access Control

The company, through its assigned executives, keeps records of all corporate resources and assets. Each information resource is under the responsibility of a specific staff-member.

The granting of rights to access information resources, follows a clear and documented procedure approved by the Top Management. Access to information resources is controlled by appropriate means and mechanisms improving security, so as the users and the devices may be identified. Users are responsible for protecting their credential to corporate information resources and fully comply to confidentiality clauses. Each device used to access corporate information is appropriately controlled. The storage media in use, are also under the company's continuous audit and are controlled.

The information the company processes either as the Controller or as the Processor and its ICT assets are classified in three (3) main classification levels and is controlled through appropriate technical measures for both; internal and external users. Access to the information resources, that are processed by the company without physical presence (remote working), is permitted through various security measures and is technically controlled.

Whenever necessary, cryptographic controls as well as pseudonymisation procedures are used.

6. CONTEXT OF THE ORGANISATION, INTERESTED PARTIES

For the effective provision of its services, the company monitors all the internal and external issues that may influence its operation, either positively or negatively, and establishes measures to prevent negative effects or achieve the essential results.

The external issues that are identified and monitored are based on political, economic, social, technological, environmental and legal aspects.

The internal issues that are identified and monitored are based on the company's value, culture, knowledge, performance and other aspects.

The Management reviews the preceding aspects and therefore, the identified issues during the annual Management Review, unless something urgent arises and needs to be discussed immediately.

The interested parties may affect the ability of the company to deliver services that meet its guests' demands and the legal requirements, so, the management analyses the needs and expectations of interested parties, and reviews this analysis during the annual Management Review meeting.

7. HUMAN RESOURCES

All the employees, according to their roles, as well as the processors, are bound to Implement Company's security policies through defined procedures in case they are processing or they are related to information resources. They are obliged to:

- Be aware of company's information security objectives and the policies and procedures related to their role;
- Implement the prescribed security procedures;
- Use the corporate information resources in accordance with their respective proper use policies and procedures that they are aware of, while they are described within the compliance manual;
- Follow the classification of information and labelling instructions;
- Transfer information according to the instructions set within the Compliance Manual;
- Always be ready to identify and report information security potential incidents;
- Fully respect the confidentiality of corporate information.

All the staff members receive the proper training in order to be able to fulfil their duties as well as the Compliance System's provisions.

8. PHYSICAL AND ENVIRONMENTAL SECURITY

Access to the corporate premises is simultaneously controlled the possible extent regarding (a) access to the premises from the external environment and (b) access to specified areas and especially the information within the premises, that are controlled against both the external and internal environment.

Access to the employees and third parties is only permitted under the appropriate authorisation and only by the use of measures specified by the company. Access to areas that are defined as of limited access is properly controlled. The company maintains specific measures to ensure physical and environmental security to the possible extent.

9. OPERATIONAL SECURITY

The corporate information systems and software are appropriately documented, with the proper updates in the event of changes and are available to all users, according to the defined needs. The company is taking measures to ensure that the systems are adequate to meet present and future business needs while taking all appropriate measures to protect systems against malware, to ensure availability of information through proper backup processes, and to fully record each operation in relevant logs for monitoring and control purposes.

10. INFORMATION SECURITY AND INCIDENT'S MANAGEMENT

All staff members, irrespective of their position in the hierarchy and their role in the company, have to immediately report any (potential) incident related to a breach in the security of the corporate information resources. Third parties (collaborators and suppliers) have a similar obligation that is described in a relevant DPA or NDA.

To this end, the company has set an appropriate security incident reporting procedure, which has been disclosed to all parties involved. Investigation of security incidents is carried out by the appropriate executives through the proper methodology, which determines, where appropriate, the security measures to be taken.

11. MANAGEMENT OF SECURITY RISKS

The company has defined by the use of state-of-the-art methodology its risks, regarding its information resources and it properly manages those risks. The methodology followed is NIST enriched methodology (NIST: National Institute of Standards and Technology of the U.S. Department of Commerce). The risks have been identified, they are continuously monitored and managed with the proper updates.

12. COMPLIANCE

The company fully complies with its obligations regarding the legal and statutory framework. It protects personal data either as Controller or as Processor having defined each situation.

Within these obligations the company fully respects the principles of lawful processing. Personal data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (principle of ‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes (principle of ‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of ‘data minimisation’);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (principle of ‘accuracy’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (principle of ‘storage limitation’);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of ‘integrity and confidentiality’).

The company fully respects all the rights of the data subjects having in place a procedure to timely answer these rights. A set of documents and a clear procedure has been implemented in order for the company to be able to timely respond requests by data subjects regarding their rights under the GDPR.

When necessary, the company implements DPIAs to achieve high level of privacy protection and fulfilment of its legal obligations.

The company has designed its System with policies, procedures and documents, in order to determine in advance and at the time of the processing itself, the means for processing by implementing appropriate technical and organisational measures.

Through the entire GDPR - ISMS the company is proving its compliance with the principles of lawful processing and the entire legal framework regarding the personal data protection.

12.1. Personal Data Protection by Design and by Default

The Company is adopting internal policies and is implementing measures which meet the principles of data protection by design and by default. The entire System's development serves this particular principle; all processes followed as well as the technical and organisational measures were re-designed to meet this principle. The company has defined the legal ground for each processing and where the legal ground is the consent of the data subject the company has set the appropriate documents in use.

The company maintains the necessary Record of Processing Activities according the legal framework.

12.2. Personal Data Retention

The company stores personal data for as long as it is required by the respective processing purpose and any other permitted linked purpose taking into consideration the relevant institutional framework.

12.3. Rights of the Data Subjects

The company fully respects all the rights of the data subjects having announced this element through its website.

13. BUSINESS CONTINUITY

In case of a variety of incidents affecting its capacity to deliver its services, the company has set a Business Continuity Management process that has been disclosed to all the involved parties. This particular part of the Compliance Manual has particular roles and functions with the aim to reduce as much as possible the interruption of the provision of its critical services according to the expectations of the interested parties and with regards to time-limits set.

14. RESUME

The company endeavours to provide consistent services which satisfy and conform to its interested parties' requirements, the legal framework under which the Company operates and the signed agreements. The company continually strengthens its position, strengthens and enhances its reputation, responds to challenges and is positively and effectively practicing in the demanding and challenging environment of its industry.

Based on the experience and know-how of its management and staff, the company aims to continuously expand services offered, focusing on quality, secure and complete satisfaction of interested parties' needs and requirements.

Confidentiality, integrity and availability of the information are in the highest level of corporate priorities. Particularly important for the company are information assets encompassing information. Being aware of the adverse impact of various threats on proper functioning, the Company through its official body, declares its commitment to continuously and comprehensively address of all issues concerning security of information. The company has set and implemented a System that complies with the entire legal framework and the ISO 27001: 2022 Standard requirements and is committed to:

- The satisfaction of interested parties by providing them high quality and secure services according to their expectations;
- Ensuring the confidentiality, integrity and availability of information processed, transmitted and maintained electronically or physically by the employees and the corporate ICT systems;
- Timely identification and response to emergencies related to breach (or suspicion of breach) regarding corporate information security or other types of interruption affecting the delivery of its services;
- Protecting the company's investment in information and communication technologies;
- Compliance with the requirements of National and European Legislation regarding its operation and the personal data management, confidentiality, copyrights and intellectual property, equality between men and women, discrimination, etc.;
- Compliance with its contractual obligations;
- Continuous improvement of the Compliance System, its efficiency and performance in terms of ensuring the quality, confidentiality, integrity and availability of information for the benefit of the enterprise itself, its employees, customers and partners.

The company ensures the resources required to support the System and support its staff with the necessary knowledge, skills and competencies on the protection of personal data and information security, utilising their skills and abilities.

The company fully recognises the objectives of the GDPR - ISMS and supports its proper implementation.

The Information Security Policy is applied for all the Hotels of the Group located in Cyprus, is available to all interested parties and is periodically reviewed so that it remains relevant and appropriate to its scope.

Radu Mitroi
Regional General Manager

Radu Stefan Mitroi
Regional General Manager
Leonardo Hotels & Resorts Mediterranean

Elena Ioannidou
Group IMS Manager

Elena Ioannidou
Health & Safety/HACCP
& Quality Group Manager

Date: 08/01/2024