Code of Conduct

Personal Data Protection

Dom Pedro Hotels & Golf Collection

Índex

1. Personal Data Protection

The protection of natural persons regarding the processing of their personal data is a fundamental right as set out in Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union.

The protection granted by the General Data Protection Regulation, hereinafter GDPR, whose present code is to be complied with, "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

This protection must be guaranteed not only by international and national authorities, but also by a person in charge in each company, who will guarantee the effectiveness of the rights of the personal data holders and ensure the scrupulous fulfillment of the GDPR.

The protection of the rights and freedoms of data holders require a division of responsibilities inside companies, so that the processing of data in each department is appropriate to the requirements of the GDPR.

The processing of personal data is done lawfully and equitably, to the extent strictly necessary to ensure information security.

The processing of data will always require the consent of the holder, except when legal obligations are involved.

It is to this extent that Dom Pedro Hotels & Golf Collection, hereinafter the Group, fulfills this Code of Conduct related with Data Protection, hereinafter Code, which aims to define the guidelines of the Group to ensure the protection of personal data, and the principles that should govern the performance of all employees.

The Group adopts policies and procedures consistent with the values it defends, and in accordance with the standards and strategies that have been taken so far.

This Code is intended to ensure that the standard values are fully disclosed within the Group and followed by all its employees so that the way to comply with the Regulation can be as effective as possible.

The Code will be a basic tool for all those who collaborate with the Dom Pedro Hotels & Golf Collection, so that it continues to act with the excellence it always presented itself.

2. Scope and Objectives

- ✓ This Code establishes the ethical and professional principles to be observed by all Group employees, in the performance of their professional duties, on behalf of the company, to comply with the GDPR.

- ✓ The purpose of this Code is to ensure that all measures taken in the Group and all policies already used guarantee the level of data protection required by the GDPR.

- ✓ The rules and procedures to be adopted in this Code are general and binding, and their non-compliance may constitute an infraction subject to disciplinary proceedings inside the Group. The infractions will be punished according to the terms established in the law.

- ✓ Data protection is a center role, and a Data Protection Officer, "DPO", is appointed to perform its duties in accordance with the law, ensuring, above all, compliance with the GDPR.

3. Rules and Procedures

- ✓ Employees, for the purposes of this Code, are those who have a working relation, internship, service or other equivalent relation with the Group.

- ✓ All Group employees who process personal data are individually responsible for compliance with applicable legal and regulatory provisions.

- ✓ Members of the Administration, in addition to being bound to comply with Data Protection rules and procedures, are responsible for implementing structures and ensuring adequate resources for the proper functioning and compliance with the GDPR rules.

- ✓ The heads of each area of the Group shall ensure that the procedures developed within their activities comply with the rules of the GDPR and have an active and dynamic role with its employees to encourage the compliance with GDPR.

- ✓ Employees are obliged to consider the confidentiality of data as an inseparable part of their duties under the contract of employment. They should also proceed in accordance with all the information and training received and comply with all the guidelines defined in the GDPR. Failure to comply with these obligations may have disciplinary consequences.

- ✓ All failures under the GDPR must be reported to the DPO.

- ✓ With the approval of the Administration, the DPO may, within the scope of its functions, determine the implementation of new measures in any area of the Group, with the support of all resources and the areas involved.

4. Personal data controllers

The entities responsible for collecting and processing Personal Data are:

Dom Pedro Investimentos Turísticos, SA,
Headquarters: Rua Dr. Fernão Ornelas nº67 2ºEsq
Postal Code: 9050-021 Funchal, Portugal
Tax Payer Number: 511013949

Dom Pedro Golf S.A.
Headquarters: Edifício Old Course - Vilamoura
Postal Code: 8125 – 406 Quarteira
Tax Payer Number: 502268808

Saviotti – Sociedade Gestora De Participações Sociais S.A.
Headquarters: Rua Dr. Fernão de Ornelas, Nº 67, 2º Esquerdo
Postal Code: 9000-055 Funchal
Tax Payer Number: 500774757

Imopedro – Sociedade Imobiliária S.A.
Headquarters: Rua Dr. Fernão de Ornelas, Nº 67, 2º Esquerdo
Postal Code: 9000-055 Funchal
Tax Payer Number: 502120606

Saviotti – Empreendimentos Turísticos S.A

Headquarters: Avenida Da República, 1910 Lote 22, Quinta Patino

Postal Code: 2645-143 Alcabideche

Tax Payer Number: 511007019

5. Data Protection Officer

- ✓ To ensure compliance with the new Data Protection Regulation, we have chosen a Data Protection Officer from the Group.

- ✓ Our Data Protection Officer is Dr. Margarida Araújo, who can be contacted to clarify any question through the e-mail address dpo@dompedro.com.

- ✓ DPO is committed to implementing the necessary measures to ensure that personal data are protected within the Group, as well as the obligation to continuously update data security measures.

- ✓ DPO is an autonomous and independent figure, whose role is focused solely and exclusively on the compliance with the GDPR. DPO does not play any other role within the Group guaranteeing a total, impartial, and no conflicts of interest performance.

- ✓ The choice of a DPO inside the Group also facilitates the effectiveness of responses to requests and complaints that may be presented by personal data holders.

- ✓ DPO is responsible for ensuring compliance with the GDPR by providing information to all employees of the Group.

- ✓ DPO is also responsible for identifying risks and suggest opportunities for improvement related to the Data Protection Policy.

6. Fundamental Principles

The recipients of this Code shall carry out their activities in compliance with the following principles:

- ✓ Legality - All measures taken and behaviors within the Group must comply with the GDPR;

- ✓ Good Faith - Relations within the Group are based on trust and correct and loyal performance, with an appropriate sense of cooperation;

- ✓ Loyalty and transparency – Personal Data must be process with lawfully, fairly and transparently in relation to the personal data holder;

- ✓ Limitation of purpose - Personal data are collected for specific and legitimate purposes and cannot be further processed in a way incompatible with those purposes;

- ✓ Minimization of data - The amount of data collected must be adequate and limited in accordance with the purposes in question;

- ✓ Accuracy - The data collected must be accurate and updated whenever necessary;

- ✓ Conservation limitation - Personal data collected must be kept only for the necessary period and for the purposes for which they are processed;

- ✓ Integrity and confidentiality - All data collected are kept securely to ensure that there are no unauthorized or unlawful access and processing of data, and to prevent accidental destruction or damage;

- ✓ Responsibility - The controller is responsible for compliance with the GDPR, and has the duty to be able to prove compliance with the Regulation by the whole Group;

7. Personal data definition

Personal data mean all information relating to an identified or identifiable person.

An identifiable person is identifiable, directly or indirectly, by reference to an identifier, which may be the name, identification number, location data (IP address), electronic identifiers (e-mail) or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

There is also a category of special data, those that reveal racial or ethnic origin, opinions, religious or philosophical beliefs, or trade union membership, as well as the treatment of genetic data, biometric data to identify a person unambiguously, health data or data relating to a person's sexual life or sexual orientation.

These data are neither treated nor collected, unless their treatment finds specific grounds in law.

8. Personal data processing

Personal data processing means any operation or set of operations on personal data, whether performed with or without automated means, such as collection, registration, organization, structuring, preservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, by broadcasting or by any other means of making available, by comparison or interconnection, as well as blocking, erasure or destruction.

Personal information should be treated according to some rules, namely:

- ✓ Always taking into account a specific and legitimate purpose;
- ✓ On the basis of a contractual and confidential relationship with the data subject;
- ✓ With the written consent of the holders of personal data;
- ✓ With the detail that is legally possible or required, according to the diversity of situations.

Any change to the method of collection and processing of personal data should be reported to the DPO to verify its feasibility and compliance with the applicable standards, and then inform the data holder.

The collection of data must be carried out for a specific purpose and be limited to the necessary information for the purpose in question and cannot relate to special categories data.
Personal data may not be used for purposes other than those for which it was collected.
It is a condition of legitimacy of treatment that the data holder is duly informed of the purpose of the treatment.

The personal data collected must be accurate and up-to-date if necessary, and inaccurate and incomplete data are erased or rectified.

If there is a need to transfer personal information and / or their measures, in particular by advising the holder of the transfer.

9. Consent

Consent is the most important information we will consider in the relations maintained between the Group and its guests and the Group and its employees.

Consent is the authorization we need to contact our guests outside the strictly commercial relationship, and with our employees, outside the strictly labor relationship.

This consent limits the performance of all the departments of the Group, in order to respect the will of the guests and employees.

For this consent to be valid it must be given freely and clarified, and it has to be possible to demonstrate it.

Informed consent presupposes that all the necessary information has been provided to the data holder to form his consent, namely the purpose of the treatment, the data to be processed, and the period of preservation of the data.

10. Personal holder's rights

Dom Pedro Group establishes procedures to protect and enforce the rights of data holders.

Some of your rights:

- ✓ The right to access your data processed by us, obtaining a copy of the data;
- ✓ The right to rectification of any inaccurate personal data concerning you;
- ✓ The right to have your personal data deleted, unless the law provides otherwise, and, in that case, to limit processing;
- ✓ Our Guests may oppose the processing of data that concerns them, for purposes associated with their circumstances, in accordance with the law;
- ✓ Data portability rights;

- ✓ Right to change the consent already given, without compromising the treatment made with the consent previously given;
- ✓ The right to be notified in the case of personal data breach;
- ✓ Right to be notified when information is stored by another method other than the original;
- ✓ Right not to be contacted for advertising, direct marketing or any other form of commercial prospecting, as well as its non-communication to third parties for the same purposes, except with the prior consent of the data holder; and
- ✓ Right to complain to any supervisory authority, or through the website of the National Data Protection Commission.

11. Employees data management

The Group complies with the requirements of labor law, namely Law no. 7/2009, of 12 February, as well as the requirements of GDPR in the management and processing of personal data of employees.

The processing of personal data is only permitted if the data processed are necessary, appropriate and proportional to the objectives to be achieved by the employer.
Employees personal data are treated not only in terms of the legislation in force, but also according to what is defined in the employment contracts.

Together with the signature of the Contract, employees are asked for their consent to:

- ✓ Collect and use image in the corporate context and outside it, for campaigns advertising and dissemination in social networks; and
- ✓ Share personal data with third parties and / or the Group, without prejudice to confidentiality, and in accordance with a specific purpose duly substantiated.

Independent consent must be obtained for each purpose, with the Group being endowed with measures and mechanisms for the conservation of the same consents, for questions of proof of legitimacy.

During the working life the employees' personal data are collected and processed for the management contractual arrangements, salary management, training procedures, absences, disciplinary procedures, work and health, biometrics control, among other procedures inherent in the provision of services.

Special category data are also processed, but only in the contractual obligations, such as occupational health and health insurance. These data are treated with confidentiality by the companies certified for the same, and covered by professional confidentiality. Human resources department does not have access to health information.

The processing of biometric data is also done, "personal data resulting from a technical processing physical, physiological or behavioral characteristics of natural person, such as facial dactyloscopic data ", in this case through fingerprint, and the treatment finds legitimacy on legal grounds, in particular for the control of attendance and security in access to certain locations.

The processing of this type of data, and its purpose are described in the contract of employment, and treatment is proportionate, necessary, justified and appropriate.

Treatment through biometric data does not violates, in itself, physical integrity of the worker, or his right to privacy.
Although we are dealing with special categories of data, the purpose of treatment is based on the need to speed up the fulfillment of an objective recognized by law as integrating control powers of the entity responsible for processing: the fixing of working control of attendance and recording of working time.

The processing of data is done through a specific program where results are collected and transferred to a data base, accessed only by the Human resources department.
In this program each employee has his own tab where it is possible to consult the accesses, inputs and outputs.
The results are stored in an encrypted database and are destroyed after the deadlines legally provided for.

The collection of personal data by the Group, and its subcontractors, are always preceded by information on the purpose of the treatment and processed in strict accordance with this purpose.

The Group assures its employees:

✓ That the treatment is carried out only within the scope of the purposes for which they were collected;
✓ That the collection, use and conservation is carried out only on the minimum personal data required and sufficient for the respective purpose;
✓ The preservation of personal data is carried out only for the period of time necessary for the

the purpose of the treatment;

✓ That there is no transmission of personal data for commercial or advertising purposes;

✓ That the processing of personal data is performed for legally foreseen purposes.

12. Employees working with personal data

All employees who treat personal data are bound by professional confidentiality and are prohibited of disclosing or using such data for other purposes.
Exceptions are made in cases where the law requires the transmission of data, particularly when required by authorities, and only in the strict field in which it is required.

These employees have an increased responsibility for the security of personal data of clients and other employees.

13. Day care

The holding of confidential information, as in the case of personal data, increases the precautions that are required, all employees should guide their performance accordingly with his responsibility.

Documents should preferably be stored on your computer, in digital folders, not in physics folders. Whenever possible, the documentation should be analyzed in digital format, to avoid unnecessary printing of documents with personal data, which when printed will become more accessible.

If it is necessary to print documents with personal data, please do not leave the documents on the printers indefinitely. An abandoned document in a printer can be easily copied, and unauthorized third parties may have access to confidential information.

It is essential that documentation is not left in places where access and consultation are possible by any person. Each one is responsible for the documentation that is in their possession.

No documentation should be kept longer than needed.
When you want to destroy documentation with personal information, this documentation must be torn.

Since many documents are stored on the computer the access to them should be restricted.

Each employee has access to his computer through a unique password. This password cannot be released by any other employee, and access to the computer should always be done exclusively by its user.

There are some cautions to take with computers namely not to let the passwords visible, don't leave documents open on your computer when you are not working, and always opt for the screen lock in an absence, even if short.
Documents should be closed whenever the user exits the computer.

Regarding copying information to storage devices, the use of these instruments and the information that is copied is controlled. The employee who wishes to copy confidential information to be used and treated outside the workplace, will have to fill a document describing the type of documentation copied, and also the reasons justifying it.
The employee will be entirely responsible for the information copied and all the risks associated.

14. Provision of data to third parties

When it's necessary to hire services to third parties (subcontractors), who may have access to personal data of customers and employees, these companies are obliged to adopt all the security measures and protocols used in the Group, with regarding the strict compliance with the GDPR.

A Data Processing Agreement is obligatorily signed, where the company undertakes to take the necessary measures to protect the confidentiality and security of personal data, as well as to prevent unauthorized access and use, loss or even unauthorized destruction of personal data.

The Group undertakes to only hire companies that present enough guarantees to protect the rights of customers and employees.

When it is a question of the fulfillment of obligations and within the functions of public interest or exercise of the public authority to which the controller is invested, there is an obligation of provision of certain personal data, within the strictly necessary for the purpose in cause.

15. Data provision at international level

The Group does not disclose personal data of its employees and guests to any third country or international organization.

It will only happen to fulfill legal obligations.

16. Data retention

According to Article 5 (1) (e) of GDPR:

"(…) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (…)"

We store data collected during the period established by law.

Tax/accounting documentation is stored for a period of 10 years in order to comply with the legal requirements.

All recruitment and selection processes are stored in the Human Resources Department during the time that the employee provides his service to the Dom Pedro Group.
After working life, and in order to comply with labor legislation, Law no. 7/2009, of February 12 and Law no. 107/2009, of September 14, the processes of employees with all personal information is stored for a period of 5 years and then destroyed.

The documentation related to clinical and health data is not stored by the Group, this obligation falls upon the company hired to manage the health insurance of employees.

No unnecessary documentation is stored.

17. Data breaches

A data breach consists of a security breach that can lead to destruction, loss, alteration, unauthorized disclosure, or improper access to personal data. This means that a data breach is more significant than the simple loss of personal data.

The violation must have effects such as discrimination, reputation threat, financial loss, loss of confidentiality or any other significant social or economic disadvantage.

All employees should be aware of what it is or what it can cause or simply allow a data breach.

Beyond the responsibility employees must have for their own behavior, is also important to be aware of any behavior that may be considered negligent by others.

More than an individual conscience it is necessary to have a global consciousness. We must be alert for possible data breaches that may occur on our side.

If documents with personal data are found in a public place, the employee who found it should try to identify the person who may have left them, as well as deliver them to the Business Center so they can stay protected until they are claimed.

It is the duty of all employees who are aware of any situation that may result in a data breach to communicate it, as a matter of urgency, to the DPO, through the address dpo@dompedro.pt, or any other more expeditious means.

When a personal data breach occurs, after a thorough review of the notification, the DPO shall communicate the situation to the National Data Protection Commission, hereinafter NDPC, within a maximum of 72 hours.

The decision to notify the violation to NDPC is the responsibility of the DPO and the Administration, who will make a case-by-case analysis to understand the type of violation, the risks and associated consequences and the measures to be taken.

This notification implies the notification of specific information. In order for the DPO to submit a complete report it is necessary that all departments of the Group as well as the employees involved are available to assist in this same report.

18. Data protection and security measures

Employees must use the material and computer resources available to them exclusively for professional purposes and diligently taking care of its maintenance, being exchange of peripherals or the opening of computer equipment prohibited without the express authorization of the Direction.

The Group has a central directory system for managing accounts and workstations of the users, with each user being assigned a user account and a password, in order to access to the available IT resources, according to their access profile.

It's from responsibility of each user to keep their passwords safe.

We have created security measures throughout the organization, namely through the creation of files and databases of data with restricted access, so that personal data do not suffer any violation, disclosure or misuse.

To protect the information you provide to us, we have implemented various security measures, including administrative, technical and physical measures.

One of the techniques that we use for online transactions is a technology called Secure Sockets Layer (SSL). If your browser supports SSL (most browsers support), your personal information will be automatically encrypted, or encoded, before it is sent over the Internet.

Dom Pedro Hotels booking engine vendor uses a Digital certificate from Rapid SSL, one of the leading providers of internet services. This certificate guarantees that your personal information is transmitted securely (encrypted) to a secure server and not to an unknown or unauthorized server.

The Group also adopts other security measures regarding the security of personal data:

- Antivirus software that provides protection against malware;
- Antivirus software that provides protection for the browser and for e-mail;
- The corporate network is protected by a firewall;
- Personal data backups are automatically enhanced;
- Our corporate Wi-Fi network is password protected;
- Remote access to our corporate network is only possible through a VPN (Virtual Private Network);
- Privileged accounts are not used for daily tasks and access to them is possible only by privileged users, and from devices dedicated and limited only to authorized persons;
- Access to sensitive personal data is controlled and limited;
- Data loss prevention software is used to protect sensitive and personal data;
- The procedures for verifying, detecting, analyzing and reporting security incidents are developed and communicated within the organization, mainly through frequent contact with the DPO;

- Personal and sensitive data are all encrypted;
- E-mail communications are encrypted;
- Folders in the Cloud / Network are encrypted.

The use of electronic mail is expressly prohibited for sending:

✓ Material that is considered illegal, including content that violates copyright or possess material that is obscene or offensive to good manners;

✓ Continuation messages intended to chain emails or equivalents.

In addition to all measures taken, the Group closely monitors all procedures through audits to confirm the compliance with GDPR.

19. Pravicy Policies

In order to comply with all the requirements of GDPR, we have updated our Data Privacy Policies, Dom Pedro Lisboa websites and Dom Pedro Golf website, as well as by creating this code that will serve as a manual for all our employees.

20. Information and Training

All information related to the GDPR, and the measures to be taken to comply with it, are made available to all employees of the Group, namely through the website.

The information is also made available through training actions developed, so that all employees can be properly informed about the GDPR and its importance.

21. Doubts and questions

In case of doubt about the application of the GDPR and the rules set forth in this Code, all employees should contact the Administration or the DPO in order to clarify any doubts as quickly as possible.
Whenever clarifications are required, the DPO should document the doubts and questions.
To all omissions in this Code will be applied the stipulated in the Regulation.