CROWNE PLAZA İSTANBUL ASIA HOTEL – VIA OTELCİLİK YÖNETİMLERİ A.Ş

PERSONAL DATA PROCESSING POLICY

1. PURPOSE AND SCOPE

The decision of the Personal Data Protection Board dated 31.01.2018 published in the Official Gazette dated 07.03.2018 Crowne Plaza Istanbul Asia Hotel - Via Otelcilik Yönetimleri A.Ş. (Via Hotel), as a data controller with the obligation to register with the Registry, is obliged to store the personal data of special nature within its body in accordance with the personal data processing inventory, to define the rules for the security of this data and to act in accordance with this policy by preparing a policy to be implemented in order to maintain it, covering all the activities to be managed.

This policy has been prepared in order to determine the procedures and principles regarding the processing, storage, transfer and security of personal data of special nature processed within Via Hotel and will be updated periodically as of the effective date.

According to Article 6 of the Law No. 6698 on the Protection of Personal Data, the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data are personal data of special nature. Different and stricter conditions are stipulated for the protection of these data than general personal data.

2. PROCESSING OF SENSITIVE PERSONAL DATA

Sensitive personal data are processed by Via Hotel in accordance with the Law, provided that adequate measures to be determined by the Board are taken, in the presence of the following conditions:

Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership to associations, foundations or trade unions, criminal convictions and security measures, and biometric and genetic data, with the explicit consent of the data subject or without seeking explicit consent in cases stipulated by law

processing is possible.

Sensitive personal data relating to the health and sexual life of the data subject may be processed with the explicit consent of the data subject, and if the data subject does not consent, only for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, by persons or authorized institutions and organizations under the obligation of confidentiality.

Within our company; as special quality data, data on criminal convictions and security measures are processed within the scope of the processing purposes detailed below, such as understanding the suitability of employees for the job and the execution of the employment contract; health data are processed within the scope of the processing purposes detailed below in order to fulfill the obligations stipulated in laws such as Labor Law, Occupational Health and Safety, or in case of extraordinary situations such as emergencies, pandemic processes. In this regard, the relevant persons are informed and, if necessary, asked whether they have explicit consent.

3. PURPOSES OF PROCESSING SENSITIVE PERSONAL DATA

Sensitive personal data;

- In cases where it is mandatory for the protection of the life and physical integrity of the person concerned as well as being expressly stipulated in the laws; in order to establish the contract and to measure the performability of the contract in order for the employer to determine the competence for the job, if the data owner is unable to disclose his consent due to actual impossibility, to carry out the processes of fringe benefits and benefits for employees and to carry out the application processes of employee candidates;
  - Health data is collected in writing from the workplace physician or the relevant person whose data is processed in accordance with the Occupational Health and Safety Law No. 6331 and the Social

Insurance and General Health Insurance Law No. 5510 and other laws for the purposes of carrying out occupational health and safety activities such as emergency management processes. The personal data in question for 15 years from the end of the legal relationship,

- Data on criminal convictions and security measures are collected from the relevant person during recruitment processes through physical, written or electronic media and stored for 10 years from the end of the legal relationship established.

- Sensitive personal data other than health and sexual life may be processed with the explicit consent of the data subject or without the explicit consent of the data subject if explicitly stipulated by law.

Sensitive personal data relating to health and sexual life may be processed without seeking explicit consent by persons or authorized institutions and organizations under the obligation of confidentiality for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

4. MEASURES REGARDING THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Within this framework, the following measures are taken by Via Otel pursuant to subparagraphs (ç) and (e) of paragraph (1) of Article 22 of the Law

- A systematic, clearly defined, manageable and sustainable separate policy for the security of special categories of personal data has been determined with this text.
- For employees involved in the processing of sensitive personal data;
  (1) Regular trainings are provided on the Law and related regulations and special categories of personal data security.
  (2) Confidentiality agreements are concluded between employees and Via Hotel.
  (3) The scope and duration of authorization of users authorized to access data are clearly defined.
  (4) Periodic authorization checks are performed once a year.
  (5) The authorizations of employees who change their duties or leave their jobs are immediately removed; in this context, the inventory allocated to them by the data controller is returned.

- If the media where special categories of personal data are processed, stored and/or accessed are electronic media;
  (1) Data is stored using cryptographic methods.
  (2) Cryptographic keys are kept in secure and different environments.
  (3) Transaction records of all actions performed on the data are securely logged.
  (4) Security updates for the environments where the data are stored are constantly monitored, necessary security tests are regularly performed and test results are recorded.
  (5) User authorizations for software used for data storage and security tests are regularly conducted against data breaches. Such test results are recorded.
  (6) If remote access to data is required, at least a two-stage authentication system is provided.
- If the environments where special categories of personal data are processed, stored and/or accessed are physical environments;
  (1) Adequate security measures are taken for a possible disaster or human events according to the nature of the environment where sensitive personal data is located.
  (2) Unauthorized entry and exit are prevented by ensuring the physical security of these environments.
- If sensitive personal data will be transferred;
  (1) If the data needs to be transferred via e-mail, it is transferred encrypted with a corporate e-mail address or by using a Registered Electronic Mail (REM) account.
  (2) If the data needs to be transferred via media such as portable memory, CD, DVD, etc., they are encrypted with cryptographic methods and cryptographic keys are kept on different media.
  (3) If the data is transferred between servers in different physical environments, the data is transferred by establishing a VPN (connecting via another IP) between the servers or by sFTP (our IP is encrypted and our identity cannot be read).
  (4) If the data needs to be transferred via paper media, necessary precautions are taken against risks such as theft, loss or unauthorized viewing of the document and the document is sent in the "Confidential Documents" format.

In addition to the measures mentioned above, technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guide published on the website of the Personal Data Protection Authority are also taken into account.

5. TRANSFER OF SENSITIVE PERSONAL DATA

Our Company may transfer the personal data and sensitive personal data of the personal data owner to third parties by taking the necessary security measures in line with the personal data processing purposes in accordance with the law in the presence of the following conditions:

- Sensitive personal data other than health and sexual life may be transferred with the explicit consent of the data subject or if explicitly stipulated by law.
- Sensitive personal data relating to health and sexual life may be transferred to persons under the obligation of confidentiality or authorized institutions and organizations for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.
- Data on criminal convictions and security measures may be transferred to authorized public institutions and organizations if stipulated by law.

In addition to the measures mentioned above, technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guide published on the website of the Personal Data Protection Authority are also taken into account.

6. RECIPIENT GROUPS

Special categories of personal data processed at Via Hotel may be shared with authorized public institutions and organizations and real persons and private law legal entities such as Workplace Physician, sworn financial advisor and persons who are obliged to keep confidentiality for the purposes and legal reasons listed herein, if requested, in case of emergencies or in case of a situation stipulated by law.

7. ENFORCEMENT

This policy has entered into force as of the date of publication and is updated annually within the framework of the procedures and principles set out above.