HOTELES
BOGOTÁ PLAZA

PERSONAL DATA PROCESSING POLICY

CONTENTS

CONTENTS

1. BASE LEGAL BASIS AND SCOPE OF APPLICATION

The information processing policy is established in compliance with Articles 15 and 20 of the Political Constitution, as well as based on Articles 17(k) and 18(f) of Statutory Law 1581 of 2012, which sets forth general provisions for the Protection of Personal Data (LEPD). Additionally, it adheres to Article 2.2.2.25.1.1, Section 1, Chapter 25 of Decree 1074 of 2015, which partially regulates Law 1581 of 2012.

This policy applies to all personal data recorded in databases subject to processing by the Data Controller.

1.1 Scope

This document applies to all personal data or any other type of information stored or used in the databases and records of HOTELES BOGOTÁ PLAZA S.A., ensuring compliance with the criteria for obtaining, collecting, using, processing, handling, sharing, transferring, and transmitting personal data. It also establishes the obligations and guidelines of HOTELES BOGOTÁ PLAZA S.A. for managing and processing personal data stored in its databases and records.

This manual applies to all HOTELES BOGOTÁ PLAZA S.A. processes that involve the processing of data (public, semi-private, private, sensitive, and data related to children and adolescents), in its role as both Data Controller and Data Processor.

1.2 Applicable Regulations

- Political Constitution of Colombia
- Law 1581 of 2012
- Decree 1074 of 2015, Chapters 25 and 26, compiling the following decrees:
  - Decree 1377 of 2013
  - Decree 886 of 2014
- Law 1266 of 2008, which establishes general provisions on Habeas Data.
- Administrative acts issued by the Superintendence of Industry and Commerce.

2. DEFINITIONS

The following definitions are established in Article 3 of the LEPD and Article 2.2.2.25.1.3, Section 1, Chapter 25 of Decree 1074 of 2015 (Article 3 of Decree 1377 of 2013).

2.1 Authorization

Prior, express, and informed consent of the Data Subject for the processing of personal data.

2.2 Database

An organized collection of personal data that is subject to processing, belonging to the same context and systematically stored for future use.

2.3 Personal Data

Any information linked or that can be associated with one or more identified or identifiable individuals. These data are classified as public, semi-private, private, and sensitive:

2.3.1 Public data

Data that is not classified as semi-private, private, or sensitive. Public data includes, among others, information related to a person's marital status, profession, occupation, or status as a merchant or public servant.

By nature, public data may be found in public records, public documents, gazettes, official bulletins, and duly finalized judicial rulings that are not classified as confidential.

2.3.2 Semi-Private Data

Data that is neither intimate, reserved, nor public, and whose knowledge or disclosure may be of interest not only to its Data Subject but also to certain groups or society in general. Examples include databases containing financial, credit, commercial, and service-related information, as well as data from foreign entities.

2.3.3 Dato privado

Personal data of an intimate or reserved nature that is of interest only to its Data Subject and requires their prior, informed, and express authorization for processing. Examples include databases containing personal phone numbers and email addresses, employment records, information on administrative or criminal infractions managed by tax administrations, financial institutions, and social security administrators, as well as databases on financial solvency or creditworthiness, personality assessments, and data managed by telecommunications service providers.

2.3.4 Sensitive Data

Sensitive data refers to information that affects the privacy of the Data Subject or whose misuse could lead to discrimination. This includes data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in labor unions, social organizations, human rights groups, or political parties, as well as data related to health, sexual life, and biometric data.

2.4 Data Processor

A natural or legal person, public or private, who, alone or in association with others, processes personal data on behalf of the Data Controller.

2.5 Data Controller

A natural or legal person, public or private, who, alone or in association with others, determines the purpose and processing of a database and/or personal data.

2.6 Person Responsible for Managing Databases

A designated employee responsible for overseeing and coordinating the proper implementation of data processing policies once data has been stored in a specific database. This role also involves enforcing the guidelines set by the Data Controller and the Data Protection Officer.

2.7 Data Protection Officer

A natural person responsible for coordinating the implementation of the legal framework for personal data protection. This individual handles requests from Data Subjects regarding their rights under Law 1581 of 2012.

2.8 Data Subject

A natural person whose personal data is subject to processing.

2.9 Processing

Any operation or set of operations performed on personal data, including collection, storage, use, circulation, or deletion.

2.10 Privacy Notice

A verbal or written communication issued by the Data Controller to the Data Subject, informing them about the existence of applicable data processing policies, how to access them, and the intended purposes of processing their personal data.

2.11 Transfer

The transfer of data occurs when the Data Controller and/or Data Processor, located in Colombia, sends personal data to a recipient, who is also a Data Controller, whether inside or outside the country.

2.12 Transmission

The processing of personal data that involves the communication of such data within or outside Colombia for a specific processing activity carried out by the Data Processor on behalf of the Data Controller.

3. PRINCIPLES OF DATA PROTECTION

Article 4 of the LEPD establishes principles for the processing of personal data that must be applied harmoniously and comprehensively in the development, interpretation, and application of the Law. The legal principles of data protection are as follows:

3.1 Legality Principle

Data processing is a regulated activity that must comply with the provisions of the LEPD, Decree 1377 of 2013, compiled in Chapter 25 of Decree 1074 of 2015, and other provisions that develop them.

3.2 Purpose Principle

Processing must serve a legitimate purpose according to the Constitution and the Law, which must be communicated to the Data Subject

3.3 Freedom Principle

Processing can only be carried out with the prior, express, and informed consent of the Data Subject. Personal data cannot be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that reveals the consent. The processing of data requires the Data Subject's prior and informed authorization through any medium that allows for later consultation.

3.4 Truthfulness or Quality Principle

The information subject to processing must be truthful, complete, accurate, updated, verifiable, and understandable. The processing of partial, incomplete, fragmented data or data that may cause errors is prohibited.

3.5 Transparency Principle

The processing must ensure the Data Subject's right to obtain from the Data Controller or the Data Processor, at any time and without restrictions, information about the existence of data concerning them. When requesting authorization from the Data Subject, the Data Controller must clearly and expressly inform them of the following, retaining proof of compliance with this obligation:

- The processing to which their data will be subjected and its purpose.
- The voluntary nature of the Data Subject's response to questions about sensitive data or data concerning children, minors, or adolescents.
- The rights of the Data Subject.
- The identification, physical address, email, and telephone number of the Data Controller.

3.6 Restricted Access and Circulation Principle:

Processing is subject to the limits derived from the nature of the personal data, the provisions of the LEPD, and the Constitution. In this sense, processing can only be carried out by persons authorized by the Data Subject and/or by those authorized by the Law. Personal data, except for public information, cannot be available on the Internet or other mass communication media unless access is technically controlled to provide restricted knowledge only to Data Subjects or third parties authorized by the Law.

3.7 Security Principle

Information subject to processing by the Data Controller or the Data Processor must be handled with the necessary technical, human, and administrative measures to ensure the security of the records, preventing their alteration, loss, unauthorized access, or fraudulent use. The Data Controller is responsible for implementing the corresponding security measures and ensuring that all personnel with direct or indirect access to the data are informed of them.

Users accessing the Data Controller's information systems must be aware of and comply with the security standards and measures relevant to their roles. These standards and security measures are included in the PL-02 Internal Security Policies, which are mandatory for all users and company staff. Any modification to the security measures for personal data by the Data Controller must be communicated to users.

3.8 Confidentiality Principle

All individuals involved in the processing of personal data that is not public in nature are obliged to maintain the confidentiality of the information, even after their relationship with the tasks involved in the processing ends. Personal data may only be supplied or communicated when it corresponds to the development of activities authorized under the LEPD and in accordance with its terms.

4. AUTHORIZATION FOR USE OF PERSONAL DATA

In accordance with Article 9 of the LEPD, the processing of personal data requires the authorization of the Data Subject, except in cases expressly established by the regulations governing data protection. Before or at the time of collecting personal data, HOTELES BOGOTÁ PLAZA S.A. will request the Data Subject's authorization for its collection and processing, clearly stating the purpose for which the data is being gathered. This authorization may be obtained through automated, written, or verbal means that allow for proof of consent to be retained, in accordance with the unequivocal conduct described in Article 2.2.2.25.2.2, Section 2, Chapter 25 of Decree 1074 of 2015.

Authorization from the Data Subject will not be required in the following cases:

- When the information is requested by a public or administrative entity in the exercise of its legal functions or by court order.
- When the data is of a public nature.
- In cases of medical or public health emergencies.
- When the processing of information is authorized by law for historical, statistical, or scientific purposes.
- When the data is related to the Civil Registry of individuals.

5. AUTHORIZATION REQUEST TO THE DATA SUBJECT

The authorization for the use and/or processing of personal data will be managed by HOTELES BOGOTA PLAZA S.A. through mechanisms that ensure its availability for future reference and confirm the consent of the Data Subject through the following means:

- In writing.
- Verbally.
- Through automated channels.
- Through unequivocal actions by the Data Subject that reasonably indicate their consent.

HOTELES BOGOTA PLAZA S.A., prior to and/or at the time of collecting personal data, will clearly and explicitly inform the Data Subject of the following:

a) The processing to which their personal data will be subjected and its intended purpose.
b) The voluntary nature of responses to questions, particularly when they concern sensitive data or data related to children and adolescents.
c) The rights available to them as a Data Subject.
d) The identification, physical or electronic address, and telephone number of HOTELES BOGOTA PLAZA S.A.

6. DATA CONTROLLER

The entity responsible for managing the databases covered by this policy is **HOTELES BOGOTA PLAZA S.A.,** whose contact information is as follows:

- **Address:** CL 100 18 A 30, BOGOTÁ D.C. - BOGOTÁ D.C.
- **Email:** mercadeo@hotelesbogotaplaza.com
- **Phone:** 300 912 9050

7. PROCESSING AND PURPOSES OF DATABASES

HOTELES BOGOTA PLAZA S.A., in the course of its business activities, processes personal data of individuals contained in databases used for legitimate purposes, in compliance with the Constitution and applicable laws. The processing of personal data includes collection, storage, use, circulation, or deletion. Data processing will be carried out in accordance with the purposes authorized by the Data Subject, contractual obligations between the parties, and any legal requirements that must be met.

Annex 2 – Database Purposes contains detailed information on the various databases managed by the company and the specific purposes assigned to each for processing.
See Annex 2 – Database Purposes

8. DURATION OF THE DATABASE

The personal data included in the databases will be retained for as long as necessary to fulfill the purposes for which their processing was authorized, in accordance with applicable regulations. Additionally, the retention period will comply with any relevant legal provisions governing data preservation.

9. RIGHTS OF DATA SUBJECTS

In accordance with Article 8 of the LEPD and Article 2.2.2.25.4.1, Section 4, Chapter 25 of Decree 1074 of 2015 (Articles 21 and 22 of Decree 1377 of 2013), data subjects are entitled to exercise several rights regarding the processing of their personal data. These rights include:

a) The right to access, update, and rectify their personal data with the Data Controllers or Data Processors. This applies to incomplete, inaccurate, outdated, or misleading data, as well as data whose processing is explicitly prohibited or unauthorized.

b) The right to request proof of the authorization granted to the Data Controller, except in cases where authorization is not required under Article 10 of this law.

c) The right to be informed, upon request, about how their personal data has been used by the Data Controller or Data Processor.

d) The right to file complaints with the Superintendence of Industry and Commerce regarding violations of this law and any other relevant regulations.

e) The right to revoke authorization and/or request the deletion of data when processing does not comply with constitutional and legal principles, rights, and guarantees. Revocation or deletion will proceed when the Superintendence of Industry and Commerce determines that the Data Controller or Data Processor has engaged in unlawful conduct.

f) The right to access their personal data free of charge, as processed by the Data Controller.

These rights may be exercised by the following individuals:

1. The Data Subject, who must provide sufficient proof of identity through the means provided by the Data Controller.
2. The Data Subject's successors, who must provide proof of this status.
3. The Data Subject's representative or legal proxy, upon proof of representation or power of attorney.
4. A third party acting under a stipulation in favor of or on behalf of the Data Subject.

The rights of minors will be exercised by their legal representatives.

9.1 Right of Access or Consultation

Data Subjects have the right to request information from the Data Controller regarding the origin, use, and purpose of their personal data.

9.2 Rights for Complaints and Claims

The law recognizes four types of claims:

- **Correction Claim:** The right to update, rectify, or modify partial, inaccurate, incomplete, misleading, or unauthorized data.
- **Deletion Claim:** The right to request the deletion of data that is inadequate, excessive, or does not comply with constitutional and legal principles, rights, and guarantees.
- **Revocation Claim:** The right to withdraw previously granted authorization for the processing of personal data.
- **Violation Claim:** The right to request corrective action for non-compliance with data protection regulations.

9.3 Right to Request Proof of Authorization Granted to the Data Controller

This right applies unless authorization is explicitly exempted as a requirement for data processing under Article 10 of the LEPD.

9.4 Right to File Complaints with the Superintendency of Industry and Commerce for Violations

The Data Subject or their successor may file a complaint with the Superintendence of Industry and Commerce (SIC) only after having exhausted the consultation or complaint procedure with the Data Controller or Data Processor.

10. PROCESSING OF MINORS' DATA

accordance with Article 7 of Law 1581 of 2012, HOTELES BOGOTÁ PLAZA S.A. processes the personal data of children and adolescents following the guidelines established in Article 2.2.2.25.2.9, Section 2, Chapter 25 of Decree 1074 of 2015 (Article 12 of Decree 1377 of 2013), while ensuring compliance with the following principles and requirements:

1. The processing of data must align with and uphold the best interests of children and adolescents.
2. The fundamental rights of minors must be fully respected in the handling of their data.

Once these conditions are met, HOTELES BOGOTÁ PLAZA S.A. will request authorization from the child's legal representative. Before granting this authorization, the minor will have the right to express their opinion, which will be considered based on their maturity, autonomy, and ability to understand the matter.

As the entity responsible for data processing, HOTELES BOGOTÁ PLAZA S.A. will ensure the appropriate handling of minors' data in accordance with the principles and obligations set forth in Law 1581 of 2012 and its regulatory provisions. Additionally, it will identify any sensitive data collected or stored to enhance security and ensure proper data management.

11. DUTIES AS DATA CONTROLLER

HOTELES BOGOTÁ PLAZA S.A., in its capacity as the Data Controller, shall comply with the following duties, in addition to any other obligations established by this law and other applicable regulations governing its activities:

11.1 Duties as data controller

a) Ensure that the Data Subject can fully and effectively exercise their right to habeas data at all times.
b) Request and retain a copy of the corresponding authorization granted by the Data Subject, in accordance with the conditions set forth in this law.
c) Properly inform the Data Subject about the purpose of data collection and their rights under the granted authorization.
d) Process inquiries and complaints submitted by the Data Subject within the timeframes established by this law.
e) Provide the Data Subject, upon request, with information regarding the use of their data.

11.2 Regarding the Data Processor

a) Ensure that the information provided to the Data Processor is truthful, complete, accurate, up to date, verifiable, and comprehensible.
b) Keep the information updated by promptly communicating any changes to the Data Processor and taking necessary measures to ensure the accuracy of the data provided.
c) Rectify any incorrect information and notify the Data Processor accordingly.
d) Inform the Data Processor if certain information is under dispute by the Data Subject, once a complaint has been filed and while the process is ongoing.
e) Provide the Data Processor only with data that has been previously authorized for processing, in accordance with the provisions of this law.

f) Require the Data Processor to uphold security and privacy standards for the Data Subject's information at all times.

11.3 Regarding Principles and Other Obligations

a) Adhere to the principles of legality, purpose, freedom, quality, accuracy, transparency, restricted access and circulation, security, and confidentiality.
b) Implement an internal policy manual outlining procedures to ensure compliance with this law, particularly regarding the handling of inquiries and complaints.
c) Notify the data protection authority in the event of security breaches that pose risks to the administration of Data Subjects' information.
d) Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.
e) Maintain data security measures to prevent unauthorized or fraudulent alteration, loss, consultation, use, or access.

12. DUTIES AS DATA PROCESSOR

HOTELES BOGOTÁ PLAZA S.A., in its role as the Data Processor, will comply with the following duties, without prejudice to any other provisions established in this law or any other applicable regulations governing its activities:

a) Ensure that the Data Subject is always able to fully and effectively exercise their habeas data rights.
b) Maintain the information under the necessary security conditions to prevent its alteration, loss, unauthorized or fraudulent consultation, use, or access.
c) Promptly update, rectify, or delete data in accordance with the terms established in this law.
d) Update the information reported by the Data Controllers within five (5) business days from the date of receipt.
e) Process inquiries and claims submitted by Data Subjects in compliance with the provisions of this law.
f) Adopt an internal manual of policies and procedures to ensure compliance with this law, particularly concerning the handling of inquiries and claims from Data Subjects.
g) Register the phrase "claim in process" in the database as stipulated in this law.
h) Insert the phrase "information under judicial dispute" in the database upon notification from the competent authority regarding legal proceedings related to the accuracy of the personal data.
i) Refrain from circulating information that is being contested by the Data Subject and has been ordered to be blocked by the Superintendence of Industry and Commerce.
j) Allow access to information only to authorized individuals.
k) Notify the Superintendence of Industry and Commerce in the event of security breaches or risks affecting the management of Data Subjects' information.
l) Comply with all instructions and requirements issued by the Superintendence of Industry and Commerce.

13. ASSISTANCE TO DATA SUBJECTS

To address requests, inquiries, and claims regarding personal data protection, HOTELES BOGOTÁ PLAZA S.A. has designated a Data Protection Officer. Data Subjects may submit their requests or inquiries through the following channels:

- **Email:** mercadeo@hotelesbogotaplaza.com
- **Address:** CL 100 18 A 30, BOGOTÁ D.C - BOGOTÁ D.C.
- **Phone:** 300 912 9050

14. PROCEDURES TO EXERCISE THE RIGHTS OF THE DATA SUBJECT

14.1 Right of Access or Consultation

HOTELES BOGOTÁ PLAZA S.A. guarantees Data Subjects free access to their personal data in the following cases, as established in Article 2.2.2.25.4.2, Section 4, Chapter 25 of Decree 1074 of 2015:

1. At least once per calendar month.
2. Whenever there are substantial changes to the data processing policies that require new inquiries.

For requests exceeding one inquiry per calendar month, HOTELES BOGOTÁ PLAZA S.A. may charge the Data Subject for shipping, reproduction, and, if applicable, document certification costs. Reproduction costs shall not exceed the actual costs of material recovery. If required, HOTELES BOGOTÁ PLAZA S.A. will provide the Superintendence of Industry and Commerce with proof of these expenses.

The Data Subject may exercise their right of access or inquiry by submitting a written request to HOTELES BOGOTÁ PLAZA S.A. via email at mercadeo@hotelesbogotaplaza.com with the subject line "Request for Access or Inquiry", or by mailing a letter to CL 100 18 A 30, BOGOTÁ D.C - BOGOTÁ D.C. The request must include:

- Full name of the Data Subject.
- A copy of the Data Subject's identification document and, if applicable, that of their representative, along with proof of representation.
- A clear and specific request detailing the information being sought.
- Contact address for notifications, date, and the applicant's signature.
- Supporting documents relevant to the request, if applicable.

The Data Subject may choose one of the following methods to receive the requested information:

- On-screen display.
- Written document, sent as a certified or regular letter.
- Email or other electronic means.
- Any other method suitable for the database system or the nature of the data processing, as offered by HOTELES BOGOTÁ PLAZA S.A.

Upon receiving the request, HOTELES BOGOTÁ PLAZA S.A. will process it within a maximum of ten (10) business days from the date of receipt. If the request cannot be processed within this timeframe, the applicant will be informed of the reasons for the delay and given a new response date, which shall not exceed five (5) additional business days beyond the initial deadline. These timeframes are established in Article 14 of the Personal Data Protection Law (LEPD).

If, after completing the inquiry process, the Data Subject or their successor is not satisfied, they may file a complaint with the Superintendence of Industry and Commerce.

14.2 Rights for Complaints and Claims

The Data Subject may submit a claim regarding their personal data by sending a written request to HOTELES BOGOTÁ PLAZA S.A. via email at mercadeo@hotelesbogotaplaza.com, with the subject line "Request for Access or Inquiry", or by mailing a letter to CL 100 18 A 30, BOGOTÁ D.C - BOGOTÁ D.C. The request must include:

- Full name of the Data Subject.
- A copy of the Data Subject's identification document and, if applicable, that of their representative, along with proof of representation.
- A detailed description of the issue and the specific request for correction, deletion, revocation, or reporting of a data protection violation.
- Contact address for notifications, date, and the applicant's signature.
- Supporting documents relevant to the claim, if applicable.

If the claim is incomplete, the applicant will be notified within five (5) business days to provide the missing information. If the required information is not submitted within two (2) months from the notification date, the claim will be considered withdrawn.

Once a complete claim is received, a note stating "Claim in Process" and the reason for the claim will be added to the database within two (2) business days. This note will remain until the claim is resolved.

HOTELES BOGOTÁ PLAZA S.A. will process the claim within a maximum of fifteen (15) business days from the date of receipt. If the claim cannot be resolved within this timeframe, the applicant will be informed of the reasons for the delay and given a new response date, which shall not exceed eight (8) additional business days beyond the initial deadline.

If, after completing the claims process, the Data Subject or their successor is not satisfied, they may file a complaint with the Superintendence of Industry and Commerce.

14.3 Authorized Individuals to Receive Information

In accordance with Article 13 of Law 1581 of 2012, HOTELES BOGOTÁ PLAZA S.A. may provide personal data to the following authorized recipients:

- The Data Subject, their successors, or legal representatives.
- Public or administrative entities performing legal duties or acting under a court order.
- Third parties authorized by the Data Subject or as required by law.

14.3.1 Verification of Authorization to Request or Receive Information

To process an inquiry or claim, the applicant must provide documentation proving their identity or legal authorization to receive the requested information, based on the following cases:

- Data Subject: A copy of their identification document.
- Successor: Identification document, death certificate of the Data Subject, proof of legal standing, and a copy of the Data Subject's identification document.
- Legal Representative or Attorney: Valid identification document, proof of representation (Power of Attorney), and a copy of the Data Subject's identification document.

15. PROCESSING OF DATA IN VIDEO SURVEILLANCE SYSTEMS

HOTELES BOGOTA PLAZA S.A will inform individuals about the existence of video surveillance mechanisms by placing visible notices within reach of all data subjects. These notices will be installed in surveillance areas, primarily at entry points to monitored locations and within these areas. The notices will provide information about the Data Controller, the purposes of the data processing, the rights of the data subjects, the available channels for exercising those rights, and where to find the Information Processing Policy.

Additionally, recorded images will be retained only for the period strictly necessary to fulfill their intended purpose. The database storing these images will be registered with the National Database Registry unless the processing consists solely of real-time image reproduction or broadcasting.

Access to and disclosure of the recorded images will be restricted to individuals authorized by the data subject and/or by request of a competent authority in the exercise of its duties. Consequently, the disclosure of collected information will be strictly controlled and aligned with the purpose established by the Data Controller.

16. SECURITY MEASURES

HOTELES BOGOTA PLAZA S.A, in compliance with the security principle established in Article 4, section (g) of the LEPD, has implemented the necessary technical, human, and administrative measures to ensure the security of records, preventing their alteration, loss, unauthorized or fraudulent access, use, or consultation.

Furthermore, through the execution of the corresponding data transmission agreements, HOTELES BOGOTA PLAZA S.A has required data processors to implement the necessary security measures to ensure the protection and confidentiality of personal data during processing.

Below are the security measures implemented by HOTELES BOGOTA PLAZA S.A, which are detailed and developed in its Internal Security Policy (Tables I, II, III, and IV).

TABLE I: Common Security Measures for All Types of Data *(public, private, confidential, restricted) and databases (automated, non-automated)*	
Document and Records Management	1. Measures to prevent unauthorized access or recovery of discarded, deleted, or destroyed data. 2. Restricted access to the location where data is stored. 3. Authorization from the Database Administrator for the removal of documents or records, whether in physical or electronic format. 4. Labeling or identification system for information classification. 5. Inventory of records.
Access Control	1. User access is restricted to only the data necessary for performing their duties. 2. A regularly updated list of users and authorized access permissions. 3. Mechanisms in place to prevent access to data beyond the authorized permissions. 4. Granting, modifying, or revoking access permissions is managed by authorized personnel.
Incidents	1. Incident log: type of incident, time of occurrence, sender of the notification, recipient of the notification, effects, and corrective measures. 2. Procedure for incident reporting and management.
Personnel	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas.
Internal Security Manual	1. Development and implementation of a mandatory compliance manual for all personnel. 2. Minimum content: scope of application, security measures and procedures, staff roles and responsibilities, database description, incident response procedures, and identification of data processors.

TABLE II: Common Security Measures for All Types of Data *(Public, Private, Confidential, Restricted) Based on the Type of Database*	
Non-Automated Databases	
Filing	1. Documentation filing must follow procedures that ensure proper preservation, location, and retrieval, allowing data subjects to exercise their rights.
Document Storage	1. Storage devices must have mechanisms that prevent access by unauthorized individuals.
Document Custody	1. The person responsible for handling documents must exercise due diligence and ensure their safekeeping during review or processing.
Automated Databases	
Identification and Authentication	1. Personalized user identification is required to access information systems, along with verification of their authorization. 2. Identification and authentication mechanisms must be in place; passwords must be assigned and have an expiration period.
Telecommunications	1. Access to data must be conducted through secure networks.

TABLE III: Security Measures for Private Data Based on the Type of Database	
Non-Automated Databases	
Audit	1. Regular audits (internal or external) conducted every two months. 2. Extraordinary audits in case of substantial modifications to information systems. 3. Report on detected deficiencies and proposed corrective actions. 4. Analysis and conclusions by the Security Officer and the Data Controller.
Security Officer	1. Appointment of one or more Database Administrators. 2. Designation of one or more individuals responsible for overseeing and coordinating the measures outlined in the Internal Security Manual. 3. Prohibition of delegating the Data Controller's responsibility to Database Administrators.
Internal Security Manual	1. Periodic compliance checks.
Automated Databases	
Access Control	1. Access control to the locations where information systems are housed.
Identification and Authentication	1. Mechanism to limit the number of repeated unauthorized access attempts. 2. Data encryption mechanisms for secure transmission.
Incidents	1. Record of data recovery procedures, including the person executing them, restored data, and manually recorded data. 2. Authorization from the Data Controller for the execution of recovery procedures.

TABLE IV: Security Measures for Sensitive Data by Database Type	
Non-Automated Databases	
Access Control	1. Access restricted to authorized personnel only. 2. Identification mechanism for access control. 3. Log of unauthorized user access attempts. 4. Destruction methods that prevent data access or recovery.
Document Storage	1. Filing cabinets, lockers, or other storage units located in secure areas with key access or other protective measures. 2. Safeguards to prevent unauthorized access or manipulation of physically stored documents.
Automated Databases	
Access Control	1. Confidential labeling system.
Identification and Authentication	1. Data encryption mechanisms for both transmission and storage.
Document Storage	1. Access log tracking: user, timestamp, accessed database, type of access, and specific record accessed. 2. Access log monitoring by the security officer.
Telecommunications	1. Data access and transmission via secure electronic networks. 2. Data transmission through encrypted networks (VPN).

17. COOKIES OR WEB BUGS

HOTELES BOGOTA PLAZA S.A may collect personal information from its users while they browse the Website, the Application, or Linked Pages (Landing Page). Users can choose to store this personal information on the website, the application, or the linked portal (Landing Page) to facilitate transactions and services provided by HOTELES BOGOTA PLAZA S.A and/or its linked portals. To achieve this, HOTELES BOGOTA PLAZA S.A uses various tracking and data collection technologies, such as first-party and third-party cookies. These analytical tools help website and application owners understand how visitors interact with their platforms. These tools may use a set of cookies to collect information and provide website usage statistics without personally identifying Google visitors.

This information allows us to understand browsing patterns and offer personalized services. HOTELES BOGOTA PLAZA S.A may use these technologies to authenticate users, remember their preferences for using the website, the application, and linked pages (Landing Page), present offers of interest, facilitate transactions, analyze website and application usage, aggregate data, or combine it with personal information in our possession and share it with authorized entities.

If a user does not wish to have their personal information collected through cookies, they can adjust their web browser preferences. However, it is important to note that if a browser does not accept cookies, some features of the website, application, and/or linked pages (Landing Page) may not be available or may not function properly. Users can allow, block, or delete cookies installed on their devices by configuring their browser settings as follows:

- **Chrome:** https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es
- **Microsoft Edge:** https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2
- **Firefox:** https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias
- **Safari:** https://support.apple.com/es-es/HT201265

18. NOTIFICATION, MANAGEMENT AND RESPONSE PROTOCOLS FOR SECURITY INCIDENTS

HOTELES BOGOTA PLAZA S.A. has established protocols for reporting incidents, ensuring effective communication and notification among employees, the Personal Data Protection Officer, data processors, data subjects, regulatory and oversight entities, and judicial authorities. These measures facilitate the timely assessment and management of identified vulnerabilities, ensuring that systems, networks, and applications remain secure.

All users, database administrators, and any individuals involved in the collection, storage, use, circulation, processing, or consultation of databases must be familiar with the procedures for responding to security incidents. This ensures the confidentiality, availability, and integrity of the information under their responsibility.

Some examples of security incidents include the failure of security systems that allow unauthorized persons to access personal data, unauthorized attempts to remove a document or record, data loss or the total or partial destruction of stored records, the physical relocation of databases, the disclosure of passwords to third parties, and the modification of data by unauthorized personnel, among others.

In the event of a security incident, the following criteria should be considered, preferably with the guidance of a Personal Data Protection advisory firm:

Strategy to Identify, Contain, and Mitigate Security Incidents

- Implement measures to contain and reverse the impact of the security incident.
- Properly assess the security incident and its impact on the Data Subjects.
- Verify legal or contractual requirements with service providers related to the security incident.
- Determine the level of risk for the Data Subjects and report the incident accordingly.
- Review the roles and responsibilities of the personnel in charge of handling the affected information or data.

Timeline for Security Incident Management

Implement guidelines for handling security incidents based on parameters that ensure proper management and impact mitigation. Based on the evaluation of the security incident, determine whether it is necessary to notify entities such as the Attorney General's Office, the Inspector General's Office, Gaula, the National Police, the Financial Superintendence of Colombia, the Cyber Police Center, COLCERT, CSIRT Police, CSIRT Asobancaria, CSIRT Sectorial, among others.

Progress of the Security Incident Report

Monitor incident management by setting deadlines, evaluating progress, and identifying potential challenges that may arise during the handling of the security incident.

Evaluation of the Response to the Security Incident

Once the security incident has been managed and controlled, review the actions taken to contain it and make the necessary adjustments to implement an improvement plan.

Implemented Actions and Improvement Plans

Define the necessary actions to mitigate the impact of the security incident and prevent recurrence through corrective and preventive measures, as well as improvement plans.

Documentation and Reporting to the Oversight Authority

Record all relevant information regarding the security incident in an internal log and prepare a report with supporting documentation of the actions taken. This report must be submitted to the Superintendence of Industry and Commerce through the RNBD within 15 business days of detecting the incident.

Review

Assess the root causes of the security incident and the effectiveness of its management to evaluate the efficiency of the controls and actions implemented. Document the lessons learned to consider them for future cases.

19. RISK MANAGEMENT ASSOCIATED WITH DATA PROCESSING

HOTELES BOGOTÁ PLAZA S.A. has identified risks related to the processing of personal data and has established controls to mitigate their causes through the implementation of its Security Policy. Therefore, the company will implement a risk management system along with the necessary tools, indicators, and resources for its administration, particularly when the organizational structure, internal processes and procedures, the volume of databases, and the types of personal data handled are considered to be exposed to frequent or high-impact events that could affect service delivery or compromise the information of data subjects.

The risk management system will assess sources such as technology, human resources, infrastructure, and processes that require protection, identifying vulnerabilities and threats to determine the level of risk. To ensure personal data protection, factors such as the type or group of internal and external individuals and different levels of access authorization will be considered. Additionally, the potential occurrence of any event or action that may cause damage—whether material or immaterial—will be evaluated, including:

- Criminal activity: Defined as actions caused by human intervention that violate the law and are subject to legal penalties.
- Physical events: Including natural and technical incidents, as well as events indirectly caused by human intervention.
- Negligence and institutional decisions: Referring to actions, decisions, or omissions by individuals with power and influence over the system. These threats are among the least predictable, as they are directly related to human behavior.

As part of its risk management program, HOTELES BOGOTÁ PLAZA S.A. will implement protective measures to prevent or minimize damages in the event of a threat materializing.

20. PROVIDING PERSONAL DATA TO AUTHORITIES

When a public or administrative entity, in the exercise of its legal functions, or a judicial order requests HOTELES BOGOTÁ PLAZA S.A. to grant access to and/or provide personal data contained in any of its databases, the legality of the request will be verified, along with the relevance of the requested data in relation to the purpose stated by the authority.

For the data disclosure, a record will be signed detailing the requesting entity's information and the characteristics of the personal data provided. This document will explicitly state the obligation to safeguard the rights of the data subject, ensuring compliance by both the requesting official, the recipient, and the requesting entity itself.

21. TRANSFER AND INTERNATIONAL TRANSMISSION OF PERSONAL DATA

HOTELES BOGOTÁ PLAZA S.A. will transfer personal data, when applicable, only to countries that provide an adequate level of data protection. A country is considered to offer an adequate level of protection if it complies with the standards established by the Superintendence of Industry and Commerce, which must not, under any circumstances, be lower than those required by Law 1581 of 2012. This restriction does not apply in the following cases:

- When the Data Subject has provided explicit and unequivocal authorization for the transfer.
- The exchange of medical data when required for the Data Subject's treatment due to health or public hygiene reasons.
- Financial or securities transfers in accordance with applicable regulations.
- Transfers carried out under international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
- Transfers necessary for the execution of a contract between the Data Subject and the Data Controller, or for the implementation of pre-contractual measures, provided the Data Subject has granted authorization.
- Transfers legally required to safeguard the public interest or to recognize, exercise, or defend a right in a judicial proceeding.

In cases where data transfer is necessary and the destination country is not listed among the "safe ports" recognized by the Superintendence of Industry and Commerce, an approval request must be submitted to obtain a compliance declaration for the international transfer of personal data.

International data transmissions between HOTELES BOGOTÁ PLAZA S.A. and a Data Processor, carried out to enable the Processor to process data on behalf of the Controller, do not require notification to the Data Subject or their consent, provided there is a data transmission agreement in place. This agreement must be signed between the Controller and the Processor, defining the scope of data processing under their responsibility, the activities the Processor will carry out on behalf of the Controller, and the Processor's obligations towards the Data Subject. Additionally, the Processor must:

1. Process personal data on behalf of the Controller in accordance with the applicable legal principles.
2. Ensure the security of databases containing personal data.
3. Maintain confidentiality regarding the processing of personal data.

The above conditions for international data transmissions also apply to national data transmissions.

22. PROCESSING OF BIOMETRIC DATA

The biometric data stored in the databases is collected and processed strictly for security purposes, to verify personal identity and manage access control for employees, clients, and visitors. Biometric identification mechanisms capture, process, and store information related to individuals' physical characteristics, including but not limited to fingerprints, voice recognition, and facial features, in order to establish or ''authenticate'' each person's identity.

The management of biometric databases is carried out using technical security measures that ensure full compliance with the principles and obligations established by the Statutory Law on Data Protection. Additionally, these measures guarantee the confidentiality and protection of the data subjects' information.

23. NATIONAL DATABASE REGISTRY – RNBD

The deadline for registering databases in the RNBD will be as established by law. Additionally, in accordance with Article 12 of Decree 886 of 2014, data controllers must register their databases in the National Database Registry on the date set by the Superintendence of Industry and Commerce, following the instructions provided by that entity. Databases created after this deadline must be registered within two (2) months from the date of their creation.

24. INFORMATION AND PERSONAL DATA SECURITY

The compliance with the regulatory framework for Personal Data Protection, as well as the security, confidentiality, and protection of the information stored in our databases, is of vital importance to HOTELES BOGOTA PLAZA S.A. Therefore, we have established policies, guidelines, procedures, and security standards, which may be updated at any time to align with new regulations and the needs of HOTELES BOGOTA PLAZA S.A. Our objective is to protect and preserve the integrity, confidentiality, and availability of information and personal data.

Additionally, we ensure that during the collection, storage, use, processing, destruction, or deletion of the provided information, we rely on technological security tools and implement security practices. These include the transmission and storage of sensitive information through secure mechanisms, the use of secure protocols, the safeguarding of technological components, restricted access to information for authorized personnel only, data backups, secure software development practices, among others.

If it becomes necessary to provide information to a third party due to a contractual relationship, we sign a data transmission agreement to guarantee the confidentiality and security of the information. We also ensure compliance with this Data Processing Policy, the information security policies and manuals, and the protocols for handling data subjects established by HOTELES BOGOTA PLAZA S.A. In all cases, we commit to the protection, security, and preservation of the confidentiality, integrity, and privacy of the stored data.

25. DOCUMENT MANAGEMENT

Documents containing personal data must be easily retrievable. Therefore, it is essential to document the location of each document, both physical and digital. Regular inspections must be conducted on these storage paths to ensure proper organization and accessibility. The preservation of these documents must be guaranteed by defining the storage medium and the conditions under which they will be kept, considering environmental factors, storage locations, potential risks, and other relevant aspects. The retention period of the documents is determined based on legal requirements, if applicable. Otherwise, each organization establishes it according to its own needs. Additionally, the final disposition of the documents must be clearly defined, whether they are to be recycled, reused, retained, digitized, or otherwise managed.

Documents related to personal data protection must be prepared by competent personnel or a qualified entity. The organization is responsible for reviewing and approving all documents, ensuring that approval is properly recorded in the designated approval section.

To facilitate traceability, documents must be properly coded and updated or modified by the responsible personnel whenever necessary. Any deletion of a document must be justified and recorded in the historical section found at the bottom of all documents.

Both physical and digital documents containing personal data must be safeguarded against external or internal threats that could alter their content, in accordance with the guidelines outlined in the Security Policy.

26. VALIDITY

This policy update will be effective as of 2025. The databases under the responsibility of HOTELES BOGOTA PLAZA S.A will be processed for as long as reasonably necessary to fulfill the purpose for which the data was collected and in accordance with the authorization granted by the data subjects.

HOTELES
BOGOTÁ PLAZA

UPDATE DATE: APRIL 2025