



P.I.A.

Top Hits Family ktv

INFOTECH 34(2018)-A (LECLAB) INFORMATION ASSURANCE &
SECURITY 1



01

PROJECT DESCRIPTION





Describe the process of the project.

The tester will collect information on the system that the business is currently using and assess based on the guideline given in the PIA template.



Objective



This project aims to test Tophits Family Ktv System and the business's conformance to legal, regulatory and policy requirements towards privacy according to the PIA template and the systems data life cycle.



P.I.A. Scope

This P.I.A. is limited to Tophits Family Ktv Dumaguete branch and its conformance to privacy in relation to their daily operation using their software system.



P.I.A. Scope

.....

Who will make decisions about the issues identified in PIA?

Tophits Management

.....

.....



P.I.A. Scope

Are there any third parties involved and how long does the system need to allow for them to play the part?

- Gcash- Until payment is confirmed (Sec-Mins)
- SMS/Call - Instant



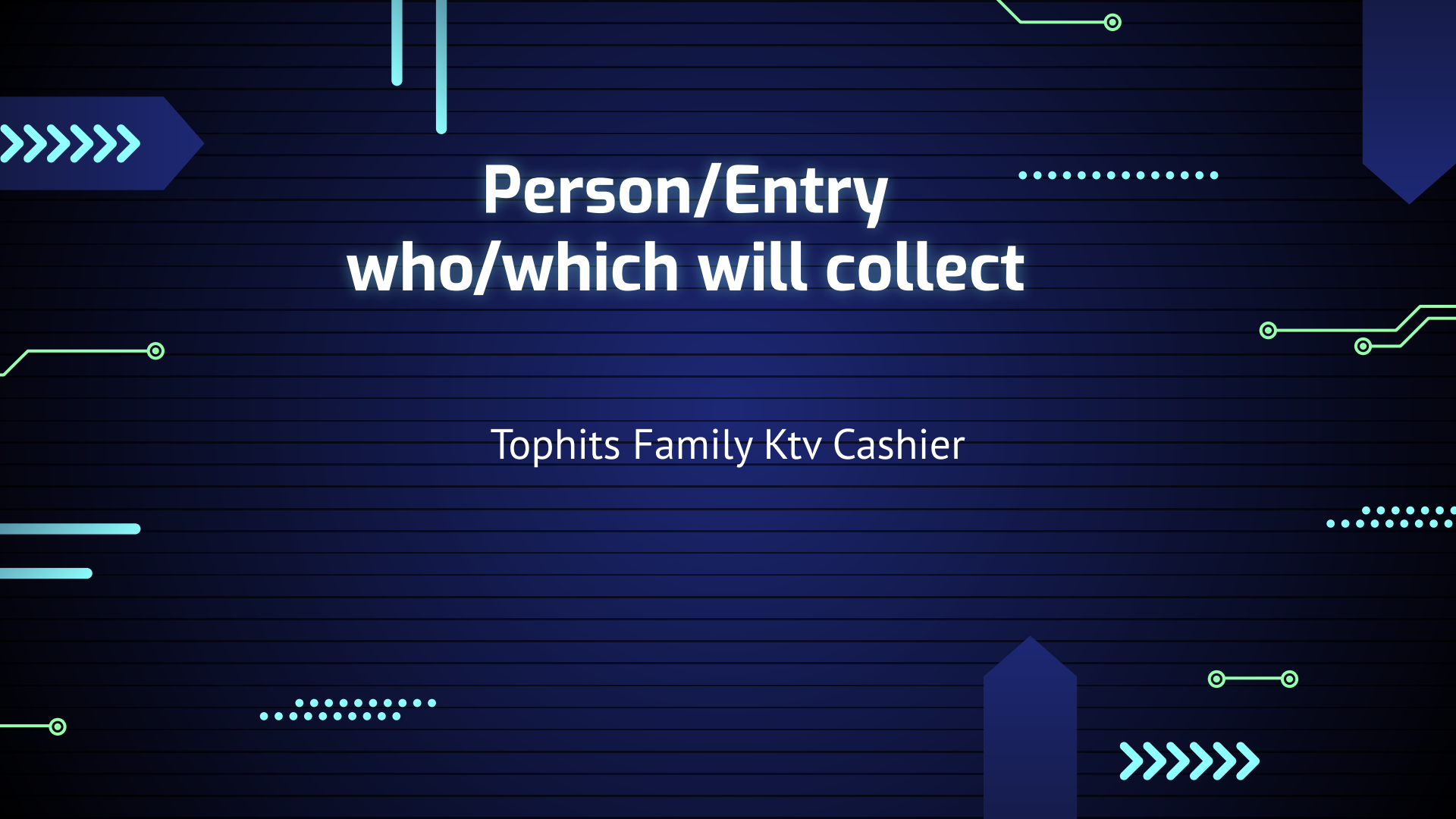
02

PERSONAL DATA FLOW



The background is a dark blue gradient with various futuristic digital elements. There are several glowing green lines and dots, some forming circuit-like patterns. On the left, there are blue arrow shapes pointing right. On the right, there are blue arrow shapes pointing left. The word "COLLECT" is centered in a large, bold, white font. The overall aesthetic is high-tech and digital.

COLLECT

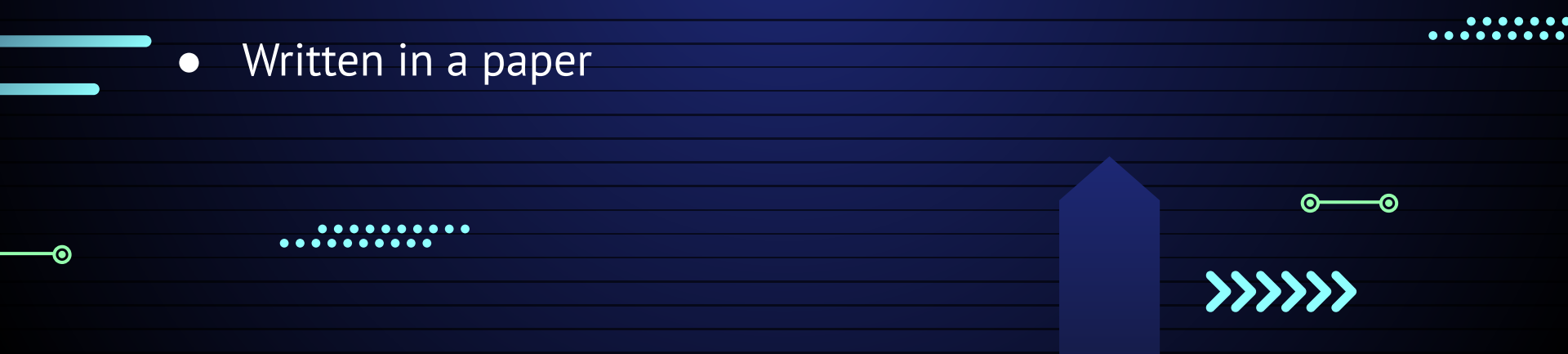


**Person/Entry
who/which will collect**

Tophits Family Ktv Cashier



How will collection be done and from who/what?

- Ask to relay information directly (call or f2f)
 - Written in a paper
- 



Purpose for collecting

To record customer name, room name, food and time of entrance for the following use:

- Schedule Booking
- Basis for karaoke 'time-end'
- Payment total

The background is a dark navy blue with various futuristic digital elements. There are several light blue geometric shapes: a large arrow pointing right in the top left, a large arrow pointing left in the top right, and two house-like shapes at the bottom. White and light blue lines and dots are scattered throughout, resembling circuitry or data paths. Some lines have small circles at their ends. The word "STORE" is centered in a large, bold, white sans-serif font.

STORE



Where will it be stored?

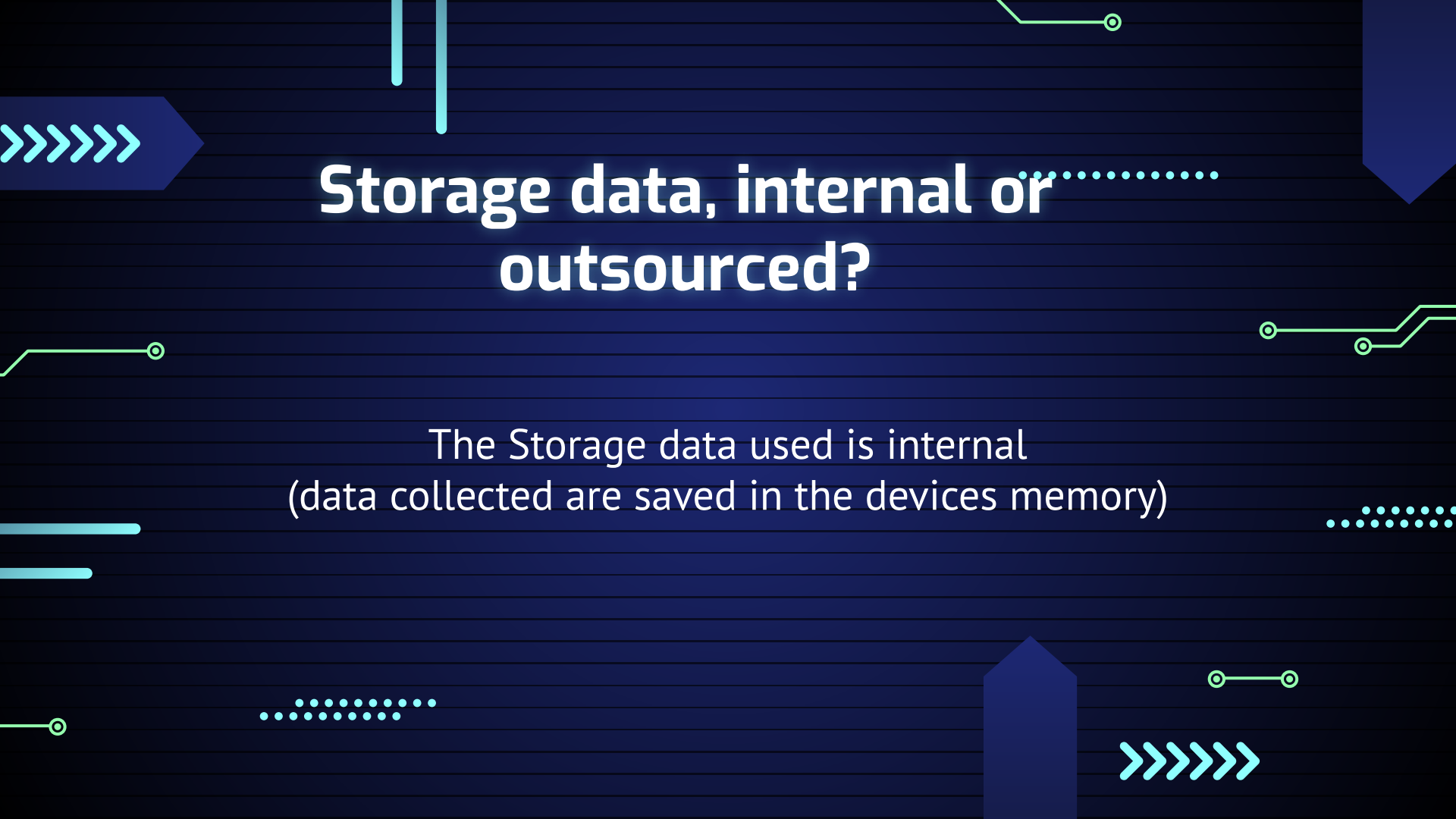
Top Hits System (hardware)



Storage within or outside Philippines?

In the Philippines.

They are located in Tophits Family Ktv, Katada Street,
Dumaguete, Negros Oriental



Storage data, internal or outsourced?

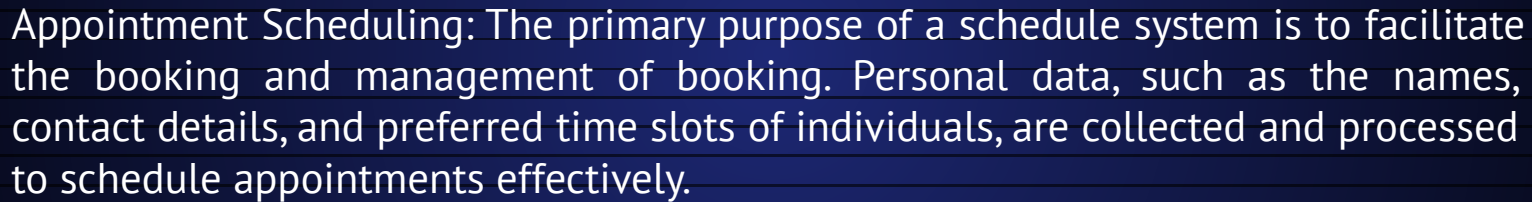
The Storage data used is internal
(data collected are saved in the devices memory)

The background is a dark blue gradient with various abstract digital elements. In the center, the word "USE" is written in a large, bold, light blue sans-serif font. Surrounding the text are several decorative elements: a large blue arrow pointing right in the top left; a series of five light blue chevrons pointing left in the top right; a series of five light blue chevrons pointing right in the middle left; a series of five light blue chevrons pointing right in the bottom left; a series of light blue dots in the top right; a series of light blue dots in the bottom right; and several light blue lines and circles resembling circuit traces or data paths scattered throughout the composition.

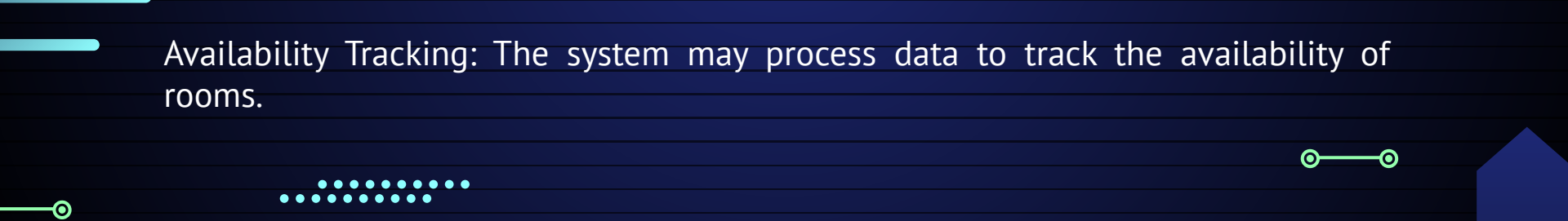
USE



Use Of Data And Purpose Of Processing



Appointment Scheduling: The primary purpose of a schedule system is to facilitate the booking and management of booking. Personal data, such as the names, contact details, and preferred time slots of individuals, are collected and processed to schedule appointments effectively.



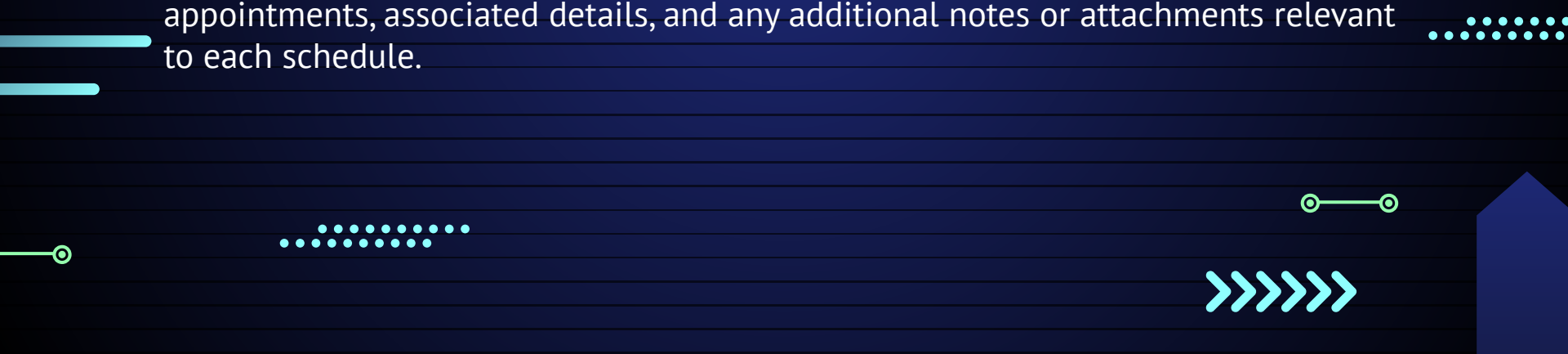
Availability Tracking: The system may process data to track the availability of rooms.





Use Of Data And Purpose Of Processing

Data Organization and Storage: The system processes data to organize and store schedule-related information. This includes maintaining records of past and future appointments, associated details, and any additional notes or attachments relevant to each schedule.



The background is a dark blue gradient with various futuristic digital elements. There are several glowing green lines and dots scattered across the frame, some forming arrow shapes pointing left or right. A prominent white line with a small circle at its end runs vertically on the left side. Another similar line runs vertically on the right side. A horizontal line with a small circle at its end runs across the middle. The word "RETAIN" is centered in a large, bold, white sans-serif font. The overall aesthetic is high-tech and digital.



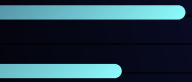
RETAIN



How Long With The Information Stay In The System?




The information will stay in the system quarterly or until a specific period for tax auditing purposes.

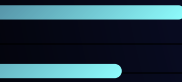





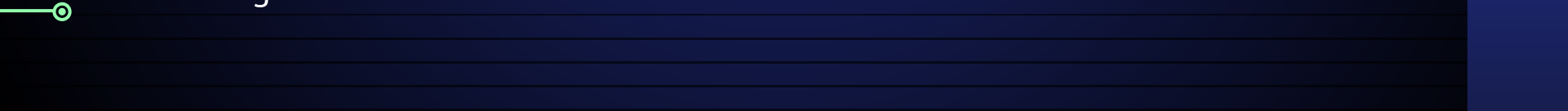
What Is Retained Internally



Scheduling Details: Internally, the system retains the details of each schedule date, such as the date, time, duration, and total payment of the schedule date. This information is necessary for managing the schedule and ensuring proper coordination.



Customer Information: The system may retain customer information internally, including names, contact details, and any additional relevant information provided by the customer during the booking process. This allows for efficient management of customer records and facilitates future communications.



What Is Outsourced?

Payment Information: If the client has already paid

Communications: SMS or calls receive from clients to book appointment and reminder for the scheduled booking.



TRANSFER or DISCLOSE

To Whom and Why?

- Staff for preparation of booked room
 - BIR- for taxation purposes

The background is a dark blue gradient with various abstract digital elements. There are several green lines of different lengths and orientations, some ending in small circles, resembling circuit traces. There are also clusters of small white dots. On the left, there are blue arrowheads pointing right. On the right, there are blue arrowheads pointing left. The word "DISPOSE" is centered in a large, bold, white sans-serif font.

DISPOSE



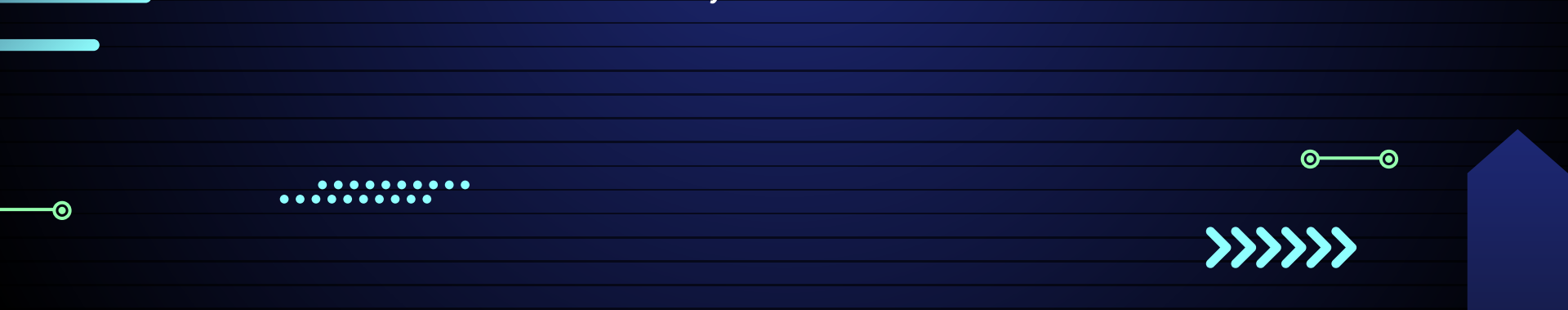
How will it be disposed?

Directly through the software










Who will dispose or facilitate disposal?

The Owner/Manager- to avoid tampering of the payment transaction
by the staff





PRIVACY IMPACT ANALYSIS

Transparency	Yes	No	Not applicable / Remarks
Are data subjects aware of the nature, purpose, and extent of the processing of his or her personal data?			
Are data subjects aware of the risks and safeguards involved in the processing of his or her personal data?			
<p>Are data subjects aware of his or her rights as a data subject and how these can be exercised?</p> <p>Below are the rights of the data subjects:</p> <ul style="list-style-type: none"> a. Right to be informed b. Right to object c. Right to access d. Right to correct e. Right for erasure or blocking f. Right to file a complaint g. Right to damages h. Right to data portability 			
Is there a document available for public review that sets out the policies for the management of personal data?			
Are there steps in place to allow an individual to know what personal data it holds about them and its purpose of collection, usage and disclosure?			
Are the data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data?			
Are the data subjects provided information about how to contact the organization's Data Protection Officer (DPO)?			

Legitimate Purpose	Yes	No	Not applicable / Remarks
Is the processing of personal data compatible with a declared and specified purpose which are not contrary to law, morals, or public policy?	/		
Is the processing of personal data authorized by a specific law or regulation, or by the individual through express consent?	/		
Proportionality	Yes	No	Not applicable / Remarks
Is the processing of personal data adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose?	/		
Is the processing of personal data necessary to fulfill the purpose of the processing and no other means are available?	/		

Data Security	Yes	No	Not applicable / Remarks
<p>Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:</p> <ul style="list-style-type: none"> a. The APIs have pre-defined parameters that must be properly filled to pass the built-in validations. b. The system is regularly tested for accuracy c. Periodic reviews of the information d. A disposal schedule in place that deletes information that is over the retention period e. Staff are trained in the use of the tools and receive periodic updates f. Reviews of audit trails are undertaken regularly. g. Independent oversight (i.e. Internal Audit) h. Incidents are reviewed for lessons learnt and systems/processes updated appropriately. 	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>		

Do you have appropriate and reasonable organizational, physical and technical security measures in place?




Organizational measures - refer to the system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing (i.e. access control policy, employee training, surveillance, etc.,)




Physical measures – refers to policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media (i.e. locks, backup protection, workstation protection, etc.,)

Technical measures - involves the technological aspect of security in protecting personal information (i.e. encryption, data center policies, data transfer policies, etc.,)



Organizational Security	Yes	No	Not applicable / Remarks
Have you appointed a data protection officer or compliance officer?		/	
Are there any data protection and security measure policies in place?		/	
Do you have an inventory of processing systems? Will you include this project/system?		/	
Are the users/staffs that will process personal data through this project/system under strict confidentiality if the personal data are not intended for public disclosure?	/		
If the processing is delegated to a Personal Information Processor, have you reviewed the contract with the personal information processor?			/

Physical Security	Yes	No	Not applicable / Remarks
Are there policies and procedures to monitor and limit the access to this project/system?			
Are the duties, responsibilities and schedule of the individuals that will handle the personal data processing clearly defined?			
Do you have an inventory of processing systems? Will you include this project/system? (may inventory of IT assets: IT asset inventory)			

Technical Security	Yes	No	Not applicable / Remarks
Is there a security policy with respect to the processing of personal data?			
Do you have policies and procedures to restore the availability and access to personal data when an incident happens?			
Do/Will you regularly test, assess and evaluate the effectiveness of the security measures of this project/ system?			

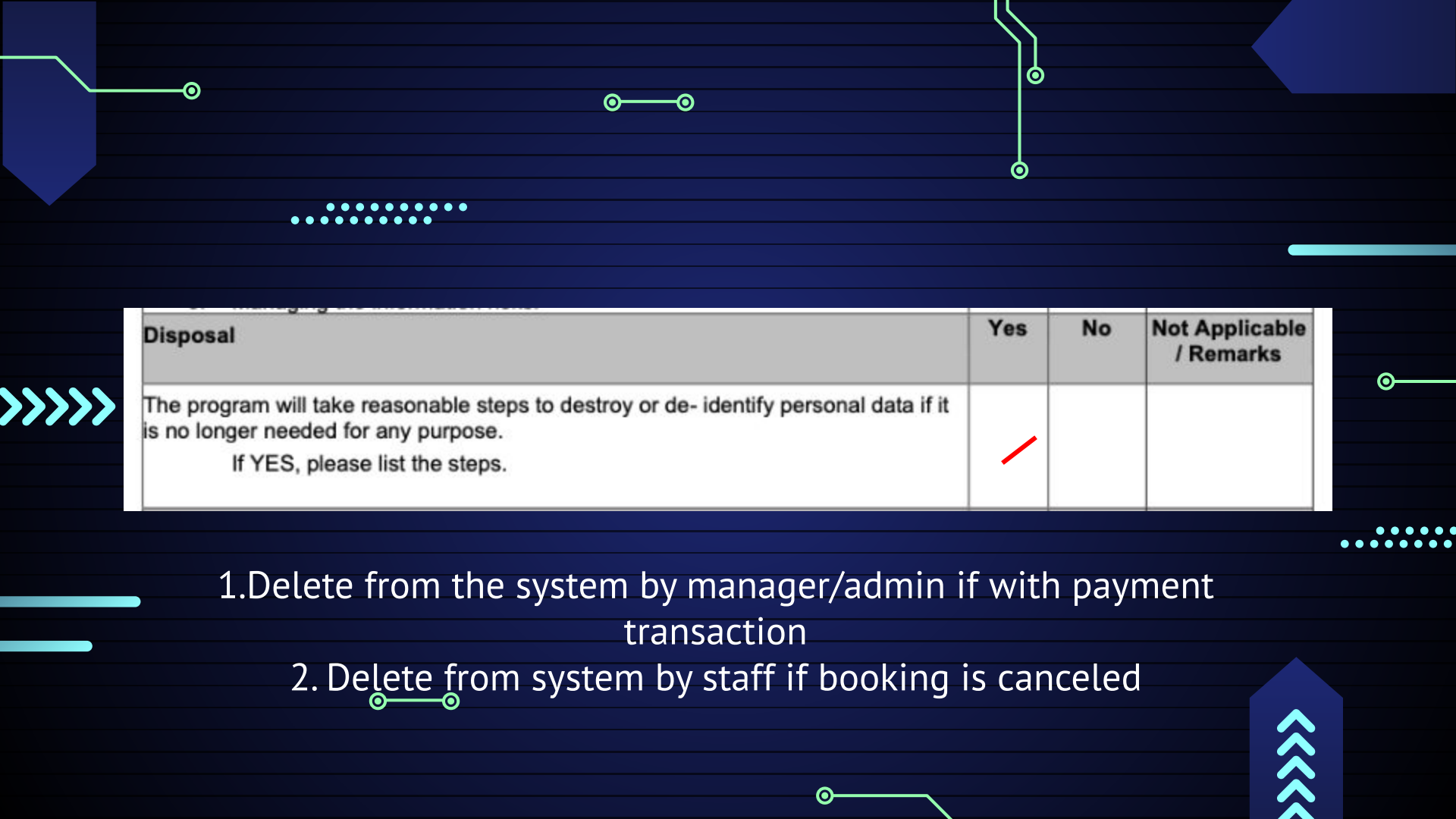
Are the personal data processed by this project/system encrypted while in transit or at rest?


The program has taken reasonable steps to protect the personal data it holds from misuse and loss and from unauthorized access, modification or disclosure?

If yes, which of the following has the program undertaken to protect personal data across the information lifecycle:



- a. Identifying and understanding information types
- b. Assessing and determining the value of the information
- c. Identifying the security risks to the information
- d. Applying security measures to protect the information
- e. Managing the information risks.





Disposal	Yes	No	Not Applicable / Remarks
The program will take reasonable steps to destroy or de- identify personal data if it is no longer needed for any purpose. If YES, please list the steps.			

- 1.Delete from the system by manager/admin if with payment transaction
2. Delete from system by staff if booking is canceled

Cross-border Data Flows (if Applicable)	Yes	No	Not Applicable / Remarks
<p>The program will transfer personal data to an organization or person outside of the Philippines</p> <p>If YES, please describe</p>			
<p>Personal data will only be transferred to someone outside of the Philippines if any of the following apply:</p> <ul style="list-style-type: none"> a. The individual consents to the transfer b. The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012 c. The transfer is necessary for the performance of a contract between the individual and the organization d. The transfer is necessary as part of a contract in the interest of the individual between the organization and a third party e. The transfer is for the benefit of the individual 			
<p>The organization has taken reasonable steps so that the information transferred will be stored, used, disclosed and otherwise processed consistently with the DPA of 2012</p> <p>If YES, please describe</p>			

Described on the video (link on last slide)

The background is a dark navy blue with various futuristic digital elements. There are several light blue geometric shapes: a large arrow pointing right in the top left, a large arrow pointing left in the top right, and two house-like shapes in the bottom corners. White and light blue lines, some with small circles at the end, suggest circuitry or data paths. A series of small white dots forms a horizontal line in the upper right and another in the lower right. In the center, the text '-END-' is written in a large, bold, white sans-serif font.

-END-

Video:

<https://drive.google.com/file/d/1DfB9ySPHC6B1aYo08ddTFAipc5rCpCz4/view?usp=sharing>