Retention: The Data the Hotel Believes It Deleted

GUIDING QUESTION *Ask your IT provider for the date of the oldest guest record that exists anywhere the hotel controls: in the property system, in backups, on old servers, in email archives, in spreadsheets, with suppliers. Then read the retention period in your policy. If you cannot get an answer to the first question within a day, your policy describes an intention, and nobody has checked whether it is carried out.*

Property: _____ Completed by: _____ Date: _____

How to use this sheet: work through the five parts with the people who own the process. The text in the left-hand columns comes from the book; the empty columns are for what is true in your property.

1. Verification Pact: what is commonly believed, what actually holds, and your property

What is commonly believed	What actually holds	In our property
«The purge function deletes old guest data.»	It deletes old data in one system. Backups, exports, old systems and suppliers keep their own copies.	
«Backups follow the retention policy.»	Only if somebody set them to. Often they keep data far longer.	
«The old system was retired after the migration.»	It was retired from daily use. Its data usually remains until somebody decides otherwise.	
«Suppliers delete our data when the contract ends.»	Only if the contract says so and somebody asks for confirmation.	
«Retention is a legal matter for the data protection officer.»	The periods are. Whether the data is actually gone is an operational and audit question.	

2. What the standard requires, and what demonstrates it

From Table 3.8.a. The third column of the book (what is method, not requirement) is left out here: write what your property actually holds as evidence.

What is required	What demonstrates it in a hotel	In our property
Information deleted when no longer required	The oldest record found in each place is within the policy's period	
Records protected in line with requirements	Periods set with the data protection officer, recorded in the information register	
Backups under an agreed policy	Backup retention matching the policy, confirmed with the provider	
Equipment verified before disposal	Old servers and laptops wiped, with a record	
Privacy requirements met	Suppliers confirm deletion at the end of a contract	
Inventory of information	Every place holding guest data listed, including retired systems	

3. The instrument: Table 3.8.b, Where the old data hides

The instrument of this subchapter. One line per place, completed during the retention audit with the oldest record actually found.

Place	What it usually holds	How the auditor looks	Question to ask
Live property system	Profiles within the purge period	Ask for the oldest profile date	Does the purge cover every table, including notes?
Backups	Every record the system ever held, for the backup period	Ask the provider for the retention setting and oldest copy	Who holds them, and for how long?
Retired systems	Everything up to the day of migration	List migrations of the last ten years	Where is the old data, and when will it go?

Place	What it usually holds	How the auditor looks	Question to ask
Exports and spreadsheets	Guest lists, rooming lists, campaign lists	Search folders and a sample of laptops by date	Who made each one, and why is it still here?
Email archives and shared folders	Attachments with guest data, years deep	Search for typical attachments and sort by date	Is there any retention on the archive?
Devices in storage	Old laptops, printers, servers	Count them and ask whether each was wiped	Where is the record of wiping?
Suppliers, current and former	Their own copies under their own rules	Written request for what is held and deleted	Did the contract require deletion at the end?

The rows above are the book's; the empty rows are for lines your property needs to add.

4. Common mistakes: self-check

Common mistake	Present here? (Yes / Partly / No)	Where we see it
Auditing retention by reading the policy and the purge setting.		
Leaving backups on a default retention longer than the policy.		
Keeping a retired system for reference without an owner or end date.		
Ignoring exports, spreadsheets and email archives.		
Never asking current or former suppliers what they still hold.		
Having nobody responsible for proving that deletion happens.		
Deleting in a panic without checking what the law and contracts require to be kept.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
List every place a copy of guest data can live, including backups, retired systems, exports, archives, devices and suppliers.			
Find and record the oldest guest record in each place.			
Compare backup retention with the policy and send any difference to the policy's owner for a decision: align the two, or justify, limit and date any longer period.			
Give every retired system an owner, an end date and changed passwords.			
Sweep the marketing, sales, events and finance folders and a sample of laptops for exports.			
Ask current and former suppliers in writing what they still hold.			
Name one person to check, once a year, where the oldest record is and why.			

Step from the book / gap found	Action in our property	Owner	Deadline
Leave the decision on what to delete to the owner and the data protection officer.			

In brief

Retention is audited by looking for old data, not by reading the policy. The internal auditor lists every place a copy can live, finds the oldest record in each, compares backups with the policy, traces every migration, sweeps the exports, asks suppliers what they still hold, and recommends that one person checks once a year. The oldest record found anywhere is the least the hotel must assume about its real retention period, and the difference between that and the policy is exposure the hotel can remove.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.8. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.