Auditing the Law Without Becoming a Lawyer

GUIDING QUESTION *Find the last internal audit report that mentions data protection and read its conclusion. If it says the hotel complies with the law, ask who in the audit was qualified to say so. If nobody was, the report has made a legal statement on the hotel's behalf, and the hotel may one day have to defend it.*

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 internal audit can confirm that the hotel complies with data protection law.»	It can confirm whether the hotel's process for meeting its obligations exists and works. Compliance with the law is a legal judgement.	
«Auditing the privacy documents audits privacy.»	Most failures are in activities (requests, deletion, notification), which documents only describe.	
«The data protection officer and the auditor do different jobs, so they need not meet.»	The auditor provides evidence the officer needs, and the officer judges what the auditor cannot.	
«A strong conclusion reassures the board.»	A conclusion beyond the audit's competence becomes evidence against the hotel when it is proved wrong.	
«The standard requires compliance with the law.»	It requires the hotel to identify its legal requirements and its approach to meeting them, and to meet them; the audit tests the approach.	

2. What the standard requires, and what demonstrates it

From Table 3.4.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
Legal and contractual requirements identified, documented and kept up to date	A register of obligations by function, each with an owner and the approach to meeting it	
Privacy and personal information requirements met	Evidence from the activities: requests handled, data deleted, contracts signed	
Compliance with policies and rules reviewed	Samples of what actually happened, compared with the hotel's own rules	
Independent review of the approach	An audit by somebody who does not run the process	
Conformity to the organisation's own requirements	Findings written in terms of the hotel's process	
Legal judgement where needed	Questions recorded and passed to the data protection officer or counsel	

3. The instrument: Table 3.4.b, The obligation trail

The instrument of this subchapter. One line per obligation, prepared with the data protection officer and completed during the audit.

Obligation, by function	Owner and approach	Evidence sampled	Question for the officer
Answer requests from individuals within the legal time	Front office manager; requests logged and tracked from any inbox, including marketing replies	Eleven requests found; two late; one never recognised	Does the ignored request need action now?
Keep personal data no longer than necessary	Revenue manager; retention periods in the register	Oldest guest profile nine years old; exports on two laptops	Are the periods set still right?
Assess every breach for notification within hours	General manager; incident plan	Four incidents logged; one not assessed	Should the unassessed one be reviewed now?
Bind processors by contract	Finance director; supplier register	Nine of eleven suppliers with contracts; two without	Are the two suppliers' own terms sufficient?
Tell guests what is done with their data	Marketing manager; notice at booking and at the desk	Notice current on the website; old version at the desk	Is the old version a problem?
Record processing activities	Data protection officer; one register shared with the system	Register matches the information register except the newsletter list	None; process finding

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
Accepting the question «are we compliant with the law?» as the scope of an internal audit.		
Comparing documents with the text of the regulation and calling it an audit.		
Auditing notices and forms instead of the activities they describe.		
Auditing without a register of obligations as criteria.		
Leaving the data protection officer out of the planning and the report.		
Looking for requests only where the privacy notice says they arrive.		
Concluding that the hotel is compliant.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Answer any request to audit legal compliance by stating in writing what the audit can and cannot establish.			
Audit whether a register of legal and contractual obligations exists, with owners and approaches.			
Sample the activities that fail most often: requests, retention, breach assessment, processor contracts.			

Step from the book / gap found	Action in our property	Owner	Deadline
Search general inboxes and contact points for requests that were never recognised.			
Agree the criteria with the data protection officer before the audit, and give the findings to the officer after it.			
Record legal questions as questions, with the evidence found, and do not answer them.			
Write findings in terms of the hotel's process, not in terms of the law.			
Never conclude that the hotel complies with, or breaches, the law.			

In brief

An internal audit examines the process that meets the law, not the law itself. It checks that the hotel has identified its obligations, assigned owners and decided how to meet them; samples the activities where obligations fail (requests, retention, breach assessment, processor contracts); searches where obligations actually arrive; passes legal questions to the data protection officer; writes findings in terms of process; and never concludes that the hotel complies with, or breaches, the law.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.4. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.