WORKSHEET 1.6

The Law and the Standard: Two Registers for the Same Hotel

Subchapter 1.6 · case in the book: Amsterdam

Ask the person who keeps your record of personal data processing, and the person who keeps your information security risk register, to tell you how long your property keeps its security camera footage. Then go and look at the recorder. If the three answers are not the same, your hotel is describing itself twice and neither description is true.

This worksheet turns the tools of the subchapter into a form you can fill in. The texts come from the book; the empty columns are for your own property. Adapt it before use: an unadapted checklist is exactly what the book warns against.

Practical application: what to do in your property

Step (from the book)	Done?	What we found / owner
Put the record of processing and the information security inventory side by side, and reconcile them line by line.		
Merge them into one register organised by process, with one owner per line.		
Check the retention configured in each system against the retention declared to guests.		
Write a short procedure for requests from guests to see, correct or erase their data.		
Assess the most sensitive processing from the guest's point of view, not only the hotel's.		
Widen the legal register to tax, registration, employment and card rules, and resolve conflicts.		
Make one list of suppliers that handle personal data, with both the legal contract and the security requirements.		
Have the data protection officer and the owner of the system meet at least four times a year.		

These steps are the book's method, not requirements of ISO/IEC 27001. Evidence can take whatever form suits the property; a separate document is needed only where an applicable requirement, or the property's own system, makes it necessary.

Verification Pact: what is believed, tested against the standard

What is commonly believed	What actually holds	Our position
«Being certified means we comply with data protection law.»	Certification shows that information security is managed. Compliance with the law is a separate question, which the system must identify and address but does not settle.	

What is commonly believed	What actually holds	Our position
«The record of processing and the asset inventory are different documents for different purposes.»	They describe the same information, systems and suppliers. Kept separately, they diverge from each other and from practice.	
«Retention is decided in the privacy notice.»	It is declared in the notice. It is decided by the configuration of each system, and the two must be checked against each other.	
«The legal register is the data protection law.»	Tax, registration, employment and card industry rules also set requirements for information, and some of them conflict.	
«Risk assessment covers privacy.»	The standard's assessment looks at risk to the organisation. The law asks about risk to the person, which can be graver, and needs to be asked explicitly.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Keeping the record of processing and the asset inventory as separate documents maintained by people who do not meet.		
Declaring retention periods in notices without checking how systems are configured.		
Assuming a certificate shows compliance with data protection law.		
Assessing risk only from the hotel's point of view, never from the guest's.		
Keeping two different lists of suppliers for law and for security.		
Limiting the legal register to data protection law.		
Letting the information security system absorb privacy and lose the questions only the law asks.		

Operative synthesis

- **The law and the standard look at the same facts and ask different questions. The law asks on what basis personal information is held, for how long and with what rights for the person; the standard asks what could go wrong with it and how it is controlled. Answered in two separate documents, both sets of answers drift from each other and from reality. Answered from one inventory, read twice, they stay true.**
- **The instrument is a single register organised by process, in which each line records the information, the systems and suppliers, the law's reading of basis and retention, the standard's reading of risk and controls, and one owner. It serves the data protection officer and the auditor from the same page, and it is what allows a hotel to answer a guest's request accurately within the time the law allows.**

- **In Amsterdam nothing had been done carelessly. A lawyer kept a meticulous record, an operations director kept a meticulous inventory, and an installer set a recorder the way recorders are usually set. Each person did their part well. The part nobody did was to check that the three of them were describing the same hotels, and the person who discovered that they were not was the guest who had the most reason to care.**
- **Which raises the question the next subchapter takes up. Every register, whether it serves the law or the standard, rests on a policy that says what the hotel will and will not do with information. What happens when that policy is written beautifully, signed at the top and impossible for anybody at the desk to check, is the case that follows.**

Action plan for our property

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 1.6. Edizioni Effedore, 2026. Clause references are paraphrased; this sheet does not reproduce the text of ISO/IEC 27001. It is not legal advice: data protection and information security law is that of the place where the property operates.