WORKSHEET 2.8

Buying Software, and the Questions Nobody Asked

Subchapter 2.8 · case in the book: Belgrade

Find the list of requirements your property used the last time it chose a major system, and count the lines that mention security, data location or how to leave. If the answer is none, the system was chosen for what it does, and the hotel will find out later what it does with the guests' information.

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
Add eight security and exit questions to the requirements for any system holding personal information.		
Put the owner of the information security system on the selection committee.		
Write data location, subcontractors, incident notice, export, deletion and change of ownership into the contract.		
Plan the migration as a change, with decisions about data, test copies and the old system.		
Test on reduced or masked data wherever possible, and delete any real test data afterwards.		
Apply retention before migrating, and move only what the hotel needs.		
Switch off and delete the old system on a planned date.		
Test a full export within the first year of any new system.		

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
«Choosing a system is about its functions.»	It is also about what the system will do with the hotel's information, and the standard asks for security requirements to be identified when acquiring systems.	
«Migration is a technical weekend.»	It is a planned change to the system that holds the hotel's guest information, with decisions about data, copies and the old system.	

What is commonly believed	What actually holds	Our position
«Testing on real data is the only way to be sure.»	Test information must be selected and protected. Real data used for testing needs the same protection as live data, and is often unnecessary.	
«We can deal with leaving when the time comes.»	Exit terms are cheap to agree before signing and expensive to obtain afterwards.	
«A reputable supplier will look after our data.»	Only the contract says where the data is, who handles it, and what happens when the supplier changes owner.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Writing requirements that describe functions and say nothing about information.		
Running the selection without the owner of the information security system.		
Treating the migration as a technical weekend rather than a planned change.		
Testing on a full copy of live data and leaving it with the integrator.		
Moving all historical data because it is simpler than deciding.		
Signing a contract that describes the start of the relationship and not its end.		
Leaving the old system running after the migration.		

Operative synthesis

- **The questions that decide how a system will treat a hotel's information are free before signing and expensive afterwards. Where the data will be, who will handle it, how the hotel will learn of incidents and changes, how it can leave and what happens to its data when it does: each is a line in the requirements, a clause in the contract and a decision in the migration plan, and each is almost always accepted by a supplier that wants the business.**
- **The instrument is a page of eight questions added to the requirements for any system that holds personal information, answered in writing and scored with the functions, together with a migration planned as a change that decides what data moves, what test copies are made and when the old system is switched off.**
- **In Belgrade nothing had been chosen badly. A committee of experienced managers scored four good suppliers carefully against two hundred and fourteen requirements and chose the best system for the hotel's work. The questions about the hotel's information were not on the list because nobody on the committee owned them, and the hotel learned the answers from a cheerful email.**

› **Which raises the question the next subchapter takes up. Some of the most sensitive information a hotel holds is not written at all. It is recorded by cameras, and in some parts of a hotel, the spa above all, the line between protecting guests and intruding on them is very fine. What happens when a camera is installed after a theft in the changing area, and nobody decides who may watch it or for how long the images are kept, 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 2.8. 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.