WORKSHEET 2.11

The First Seventy-Two Hours

Subchapter 2.11 · case in the book: Barcelona

Suppose that at five on a Friday afternoon an email arrives at your property's general address, claiming to hold your guests' data and attaching fifty real records as proof. Write down who will read it, when, who will decide whether it is true, and who will decide whether the authorities and the guests must be told. If the answers begin on Monday, the clock will have run for three days before anybody looks at it.

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
Make sure every address and number through which a warning might arrive reaches the duty manager at any hour.		
Name the decision-maker at any hour, with deputies, and put the names and numbers on one page.		
Give the duty manager five questions for the first hour.		
Teach everybody: do not forward, do not reply, do not delete.		
State in the plan when the legal clocks start and what each requires.		
Agree who speaks for the hotel, and give every guest-facing team the same holding statement.		
List copies of guests' data held by suppliers, so the investigation knows where to look.		
Rehearse the plan once a year with a realistic scenario.		

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
«The clock starts when we have confirmed the breach.»	Where the data protection regulation applies, it runs from becoming aware, which does not wait for certainty.	
«Forwarding the email to everybody concerned is the right thing to do.»	It spreads the data and the evidence. The original is kept and sent only to the people the plan names.	

What is commonly believed	What actually holds	Our position
«The general manager decides.»	Somebody must decide at any hour, including when the general manager is away. The plan names who.	
«If the data was taken from a supplier, it is the supplier's breach.»	The hotel remains responsible for guests' data it gave to a supplier, and its own obligations still apply.	
«Staff should answer guests' questions honestly.»	They should, and they should all give the same answer, which the hotel decides and gives them.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Letting warnings arrive at a mailbox nobody reads at weekends.		
Leaving it unclear who decides when the general manager is away.		
Having no quick way to judge whether an event is a breach.		
Forwarding the original message widely, or replying to the sender.		
Believing that the clock starts only when the breach is confirmed.		
Letting every guest-facing team improvise its own answer.		
Forgetting the copies of guests' data held by suppliers.		

Operative synthesis

- **The first seventy-two hours of an incident are decided before it starts: by where warnings arrive and who reads them, who decides at any hour, how an event is judged, how evidence is kept, when the legal clocks start, who speaks for the hotel and where copies of the data are held. Prepared, they are hard; unprepared, they are chaotic, and the chaos is visible to guests, authorities and the press.**
- **The instrument is a two-page plan: names and numbers, five questions for the first hour, three things not to do, and a timeline for the first hour, the first day and the first seventy-two hours. Kept at the desk and on the duty manager's phone, and rehearsed once a year, it gives the hotel one voice and a clear head when it needs them most.**
- **In Barcelona nothing had been done carelessly. A reservations agent recognised a regular guest's name and raised the alarm, a deputy general manager tried to tell everybody who might need to know, and a data protection officer notified within seventy-two hours of the hotel reading the email. The warning had sat unread for a weekend, the hotel had no single person to decide, and the data had been taken from a copy nobody remembered giving away.**
- **Which raises the question the next subchapter takes up. Some incidents begin with a demand; others begin with a delegate in a conference session running a program on the hotel's own Wi-**

Fi. What happens when the network guests use and the network that runs the hotel turn out to be the same, 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 2.11. 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.