

## **Title**

Data Protection in the Hospitality Sector: Industry Specificities and Regulatory Challenges

## **Brief Overview**

The hospitality sector processes large volumes of sensitive personal data, making compliance with data protection law a critical component of risk management and reputation governance.

Operational areas such as guest registration, loyalty programmes, video surveillance, marketing, and IT systems pose heightened compliance risks. Hotels must adopt structured governance, clear responsibilities, and robust technical safeguards to ensure lawful processing and protect trust.

## **Practice Group**

Data Protection & Privacy

Hospitality & Tourism Law

Compliance & Regulatory Advisory

Cybersecurity & Risk Management

## **Full Article**

In contemporary business operations, data protection is no longer merely a matter of compliance with statutory requirements, but an integral component of risk management and reputation governance. In the hospitality sector, this issue is further complicated by the nature of the services provided and the volume of personal data processed on a daily basis.

A hotel is not merely a provider of accommodation services – it is simultaneously a controller of a significant amount of identification, financial and security-related data, the processing of which must be carefully structured and legally grounded. In this respect, the hospitality sector represents one of the industries in which commercial data processing, statutory obligations and security requirements intersect.

## **Personal Data Processing Operations in the Hospitality Sector**

The hospitality sector involves a complex structure of personal data processing encompassing various processes, purposes and legal bases. Within a single business system, contractual processing (reservation and accommodation), statutory record-keeping obligations, security measures, marketing activities and cooperation with numerous partners operate simultaneously.

Data protection in this sector therefore requires a systematic analysis of each individual process, including:

- reservation processes (directly or through intermediaries),
- guest check-in and check-out procedures,
- record-keeping in accordance with applicable local regulations,
- processing within loyalty programmes,

- marketing communications,
- the use of video surveillance systems,
- cooperation with service providers and other business partners.

Regulatory practice in Europe shows that these operational processes are most frequently subject to supervisory scrutiny. Particular attention is given to issues of excessive data collection, unclear legal bases for processing, insufficient transparency towards guests, as well as inadequate technical and organisational security measures.

### **Where Non-Compliance Most Commonly Arises in Practice**

Although the fundamental principles of data protection are clearly defined at a normative level, irregularities in practice most often arise in operational segments of business activity, where speed and efficiency tend to take precedence over legal assessment. Regulatory practice indicates that the following areas are particularly high-risk:

#### **1. Guest Registration and the Principle of Data Minimisation**

One of the key issues concerns the scope of personal data collected during guest check-in. Although hotels are subject to statutory obligations regarding the recording of certain guest information, such obligations cannot automatically justify copying or retaining the full content of identification documents where no clear and proportionate necessity exists. The principle of data minimisation requires that only data strictly necessary for a specific purpose be collected, and that retention periods be defined in advance. In practice, the absence of a clear assessment of “why” certain data are required and “for how long” they are retained frequently constitutes the basis for findings of non-compliance.

#### **2. Marketing Activities and Loyalty Programmes**

Loyalty programmes and direct communication with guests represent an important component of the hotel business model. However, regulatory practice shows that marketing activities are a common source of non-compliance – particularly in situations where there is no clear legal basis for sending promotional communications, where opt-out mechanisms are not straightforward, or where personal data are retained for marketing purposes without clearly defined retention periods. Processing for marketing purposes must be clearly distinguished from processing that is necessary for the performance of the accommodation contract, both in documentation and in the technical implementation of relevant systems.

#### **3. Video Surveillance and the Exercise of Data Subject Rights**

The use of video surveillance systems for the protection of property and guest safety entails data processing that carries specific risks. Particularly sensitive issues include the determination of retention periods for recordings, restrictions on access, and the handling of data subject access requests. In practice, irregularities most often arise due to excessively long retention periods,

insufficiently defined internal procedures, or inadequate balancing between the rights of the requesting individual and the rights of other persons who may appear in the recordings.

#### **4. Cybersecurity and Incident Management**

In recent years, the hospitality sector has been affected by serious security incidents involving the compromise of large volumes of guest data and disruptions to information systems. Supervisory authorities have, in certain proceedings, emphasised that technical and organisational security measures must correspond to the risks arising from the scope and nature of the processing activities. A particular challenge lies in the reliance on centralised systems and external IT support, whereby the controller's responsibility does not cease merely because a system has been developed or maintained at group level or by a third party.

#### **5. Complexity of the Processing Chain and Allocation of Responsibilities**

Hospitality operations are rarely confined to a single legal entity. Reservations are made through platforms, data are exchanged with central offices and franchise structures, and IT systems are maintained by external providers. Such a structure increases the risk of ambiguity regarding roles (controller, joint controller, processor) and the allocation of responsibility in the event of a personal data breach. In practice, insufficiently precise contractual arrangements and the absence of a clearly defined division of responsibilities often create an additional layer of risk.

### **Data Protection as an Element of Sustainable Business Operations**

Data protection in the hospitality sector does not constitute a secondary regulatory issue, but rather one of the key areas of legal risk and corporate responsibility. The specificity of the sector lies in the large volume of identification data processed, continuous real-time processing activities and a complex chain of actors involved in the processing.

A hotel seeking long-term business stability must view data protection as an integral component of its operational structure – from front desk operations to IT departments, from marketing functions to security management. Otherwise, the risk extends beyond potential regulatory sanctions and directly affects the trust that is of fundamental importance in this industry.

*This article is to be considered as exclusively informative, with no intention to provide legal advice. If you should need additional information, please contact us directly.*

#### **Author:**

Sonja Stojčić  
Senior Associate