MASTER IN
Law &
Management

The Limits of Data Disclosure in Hotel M&As Transactions

Camila Belén Erazo Prado

Supervisor

José Ferreira Gomes

April 2025

The Limits of Data Disclosure in Hotel M&As Transactions

Os limites da Divulgação de Dados nas Transacções de Fusões e Aquisições de Hotéis

Camila Belén Erazo Prado[1]

camilaerazop@gmail.com

ABSTRACT

This thesis investigates the legal and practical limits of data disclosure in hotel mergers and acquisitions within the European Union, focusing on Portugal and Spain. It analyzes evolving regulatory frameworks, industry-specific challenges, and the impact of emerging technologies, highlighting the importance of due diligence and compliance for effective and secure M&A transactions.

KEYWORDS

Merger and acquisitions; disclosure; hospitality; data privacy; GDPR.

RESUMO

Esta tese investiga os limites legais e práticos da divulgação de dados em fusões e aquisições de hotéis na União Europeia, centrando-se em Portugal e Espanha. Analisa a evolução dos quadros regulamentares, os desafios específicos do sector e o impacto das tecnologias emergentes, salientando a importância da diligência devida e da conformidade para a eficácia e segurança das transacções de fusões e aquisições.

PALABRAS-CHAVE

Fusões e aquisições; divulgação; privacidade dos dados; hotelaria; GDPR.

[1] Thesis in Law presented by the student as a requirement to obtain the master of Law & Management from Law School of Universidade de Lisboa (FDUL), with collaboration with Instituto Superior de Economia e Gestão (ISEG).

ABBREVIATIONS

ADR Average Daily Rates

AEPD Spanish Data Protection Agency

BDSG Germany's Federal Data Protection Act

BGH German Federal Court of Justice

CCPA California's Consumer Privacy Act

CEHAT Spanish Confederation of Hotels and Tourist Accommodation

CFREU Charter of Fundamental Rights of the European Union

CNPD The Portuguese Data Protection Authority

DPOs Data Protection Officers

EBITDA Earnings Before Interest, Taxes, Depreciation, and Amortization

EDPB European Data Protection Board

EEA European Economic Area

EU European Union

FSB Financial Stability Board

GDPR EU General Data Protection Regulation

HMA Hotel Management Agreement

ICO UK Information Commissioner's Office

M&A Mergers and Acquisitions

NDAS Non-Disclosure Agreements

PCI DSS Payment Card Industry Data Security Standard

Pets Privacy Enhancing Technologies

PIPL China's Personal Information Protection Law

RevPar Revenue per Available Room

SCCS Standard Contractual Clauses

SPA Share Purchase Agreement

TABLE OF CONTENT

1 Introduction

Hospitality mergers and acquisitions (M&A) are becoming increasingly prevalent in today's globalized market, driven by industry consolidation and the pursuit of strategic synergies. However, the processing of personal and commercial data by hotels, in addition to the cross-border nature of numerous operations, introduces a unique degree of complexity to these transactions. The absence of harmonized protocols and the simultaneous management of sensitive personal information creates a problem that needs to be addressed by authorities for data privacy surveillance.

The digital transformation of the hospitality sector has increased the strategic value of customer data, making data protection not only a matter of regulatory compliance but also a core operational imperative and a competitive differentiator. In this context, the boundaries of lawful data disclosure have become a critical concern, especially as hotels must reconcile the need for transparency in M&A with stringent privacy obligations under frameworks such as the General Data Protection Regulation (GDPR) and national laws.

Despite the extensive literature on mergers and acquisitions (M&A) and on data privacy as separate domains, there is a notable gap in academic research addressing their intersection within the hospitality industry. This thesis addresses this gap by systematically analyzing the theoretical and regulatory boundaries of data disclosure in hotel M&A transactions, with a particular focus on the evolving legal landscapes of Portugal and Spain. These jurisdictions have recently implemented significant regulatory changes (Portugal's Law 58/2019 and Spain's Royal Decree 933/2021) that exemplify the complexities and compliance burdens faced by international hotel operators.

In this thesis, the topic will be examined in the context of pre-transaction due diligence. This component is of the utmost importance, as it plays a pivotal role in safeguarding data and ensuring the successful outcome of the M&A transaction. Mergers and acquisitions are complex phenomena that require a comprehensive understanding of theoretical knowledge. For investigation purposes, I will assume that the transactions in question are common and general, necessitating a detailed analysis of each specific situation.

The primary objective of this research is to delineate the legitimate limits of data disclosure in hotel M&A transactions, identifying both the legal principles and the practical mechanisms that

govern information exchange. The central research question guiding this study is: What are the limits of data disclosure in hotel M&A transactions under EU, Portuguese, and Spanish law?

In order to address the topic, the thesis employs a multidisciplinary approach, integrating legal analysis, economic theory, and insights from the field of hospitality management. The structure of the thesis is as follows: first, it reviews the relevant legal frameworks and theoretical foundations; second, it examines the specific categories of protected hotel data and their disclosure thresholds; third, it analyzes the practical implementation of disclosure limitations in M&A processes; and finally, it offers recommendations for the further research or applications.

By clarifying the limits of data disclosure in hotel M&A transactions, this thesis aims to contribute both to academic doctrine and to the development of effective compliance strategies for practitioners. The findings are intended to inform future regulatory developments and to support the sustainable growth of the hospitality sector in an increasingly data-driven and regulated environment.

2 Theoretical Framework: Data Privacy in M&A

2.1 Origins of Data Privacy Protection

Privacy rights are a concept that has emerged from philosophical debates concerning individual autonomy and transparency. In 1890, Warren and Brandeis articulated the "right to be let alone" in their article; establishing a legal precedent that would serve as a safeguard against the encroachment of intrusive technologies.[2] Sweden was the first nation to establish a legal response to systemic data governance challenges. The Swedish Data Act of 1973 was instrumental in achieving this objective. The act established the principles of data protection, which have served as a foundation for subsequent developments in this field.[3]

By the 1980s, the European Union's legal framework was facing significant challenges from the rapidly expanding market of the United States. In 1981, the Council of Europe Convention 108 established a set of regulations pertaining to the cross-border transfer of data[4]. The concepts of personal data processing and legitimate interest were introduced to define the principles of purpose

[2] WARREN AND BRANDEIS, 1890. *About the authors, these two scholars, representing the United States, have emerged to trace the growth of data protection law, focusing on developing the topic until its codification.*
[3] FREESE, 1978.
[4] INTERNATIONAL NETWORK OF PRIVACY LAW PROFESSIONALS, 2018.

limitation and data minimization during the publication of the Data Protection Directive 95/46/EC[5].

The constitutions of each member state of the European Union include provisions for the recognition of data protection rights and the establishment of national data protection authorities. The purpose of these provisions is to enhance the accuracy and promulgation of data protection legislation[6]. In May of 2019, the General Data Protection Regulation (GDPR) was implemented, resulting in the refinement of pertinent concepts and the establishment of a unified enforcement framework.

Despite the presence of certain deficiencies and ambiguities within the judicial system, EU rules have proven beneficial in addressing challenges related to emerging technologies. However, the continuous growth of innovation necessitates the ongoing formulation of guidelines for the practice of law.

2.2 The Legal Theory of Data Protection as a Fundamental Right

The conceptualization of data protection as a fundamental right signifies a substantial evolution in legal theory, particularly within the European context. This elevation carries profound implications for M&A transactions, where the handling of personal data must now be regarded not merely as a matter of regulatory compliance, but as a matter of fundamental rights protection.

The Lisbon Treaty's of 2009, signified a pivotal moment in the realm of data protection; the treaty established data protection as a fundamental right within the EU legal order, together with the right to privacy.[7]

The European Union has explicitly recognized the protection of personal data as a fundamental right, distinct from the traditional right to privacy. Article 8(1) of the Charter of Fundamental Rights of the European Union (CFREU) expressly guarantees the right to the protection of personal data concerning any individual.[8] This separation is significant because it establishes data protection as an independent right that merits constitutional level protection, rather than simply as a subset of privacy concerns.

---

[5] (1995) Directive 95/46/EC, *on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Final 2018.
[6] ERDOS, 2019: 35-54.
[7] TZANOU, 2013: 88-99.
[8] (2000) Charter of Fundamental Rights of the European Union (2000/C 364/01): Article 8.

This classification is predicated on the recognition that contemporary data processing engenders unique risks that may not be adequately addressed by traditional privacy frameworks. Jurists position on this issue is that data protection has become detached from the right to privacy in EU legislation and has been designated a fundamental right.[9]

The German Constitutional Court's influential decision on informational self-determination has significantly shaped this theoretical approach, establishing that individuals should maintain control over the disclosure and use of their personal data.[10] This right is based on constitutional protections of human dignity and personality rights, and requires clearly defined conditions of processing to ensure that individuals are not reduced to mere objects of information in an era of automated data collection and processing.[11]

The EU General Data Protection Regulation (GDPR) operationalizes this fundamental right through a comprehensive system of principles, rights, and obligations that significantly impact M&A transactions. Data protection is emerging as a fundamental right that specifically addresses the power imbalances created by modern data processing technologies.[12]

2.3 Data Privacy as a Non-Price Competition Parameter

A non-price competition parameter is any factor, other than price, that a company uses to attract customers and gain an advantage over other companies in the market. In markets where there is imperfect competition, these factors are very important. In these markets, companies try to stand out from their competition by offering something other than low prices.[13]

Beyond its status as a fundamental right, data privacy has increasingly been recognized as a significant non-price parameter of competition. The notion of privacy as a competitive parameter challenges traditional economic models that prioritize price effects. As marketplaces continue to evolve, particularly in the digital sector, a growing consensus has emerged that the level of privacy protection and the deployment of Privacy Enhancing Technologies (PETs) could become subject to competition from private companies. This perspective does not conceptualize privacy

[9] About this topic, LEENES ET AL., 2017.
[10] The 1983 Census Judgment, also referred to as the "*Volkszählungsurteil*," is widely recognized as a pivotal ruling by the German Federal Constitutional Court. This judgment significantly influenced the theoretical framework of informational self-determination, thereby establishing a foundation for the subsequent development of related concepts and practices.
[11] TZANOU, 2019, 88-99.
[12] RODOTÁ, 2009: 77.
[13] SACHÁ, 2021.

exclusively as a regulatory constraint; rather, it is regarded as a quality dimension of products and services that firms can leverage for competitive advantage.[14]

"The European Commission acknowledges that data privacy constitutes a key parameter of non-price competition in the market for consumer communications […]."[15] This recognition has profound implications for our understanding of privacy in competitive markets, positioning it as a potential quality dimension that consumers value and that companies can strategically enhance. The implications are significant for M&A transactions in the hospitality industry. If privacy practices represent a competitive advantage, then the acquisition of companies with strong privacy governance might command premium valuations. Conversely, privacy deficiencies identified during due diligence might justify price reductions or specific contractual protections.[16]

The European Commission's acknowledgement of data privacy as a non-price competition parameter is evident in its merger control decisions, particularly in the Microsoft/LinkedIn case.[17] The Commission has made it clear that privacy standards are a key parameter of competition for professional social networks, impacting user choice and service quality.[18] This aligns with the broader EU framework, where privacy is increasingly recognized as a quality dimension in digital market assessments.[19]

The OECD further reinforces this theoretical perspective, noting that: "when consumers and users are also data subjects, and data play a pivotal role in platforms' market power, data privacy could become a relevant non-price parameter of competition, whether as a dimension of quality or of choice."[20] This observation is particularly relevant to the hotel industry, where guest data has become a central competitive asset.

In M&A contexts, this theoretical framework also creates tensions. While full information disclosure during due diligence may be required to accurately assess the value of privacy related competitive advantages, such disclosure can potentially compromise the very privacy protections that are essential to those advantages.

---

[14] ESAYAS, 2018.
[15] Ibidem.
[16] EUROPEAN COMMISSION, 2024. *Directorate General for Competition; Protecting Competition in a Changing World.* 34.
[17] EUROPEAN COMMISSION, 2016. Case n. M.8124 – Microsoft v. LinkedIn.
[18] EUROPEAN COMMISSION, 2024. Directorate General for Competition., Non-Price Competition.
[19] EUROPEAN DATA PROTECTION BOARD, 2025. *Position paper on Interplay between data protection and competition law.*
[20] OECD, 2025. *The Intersection between Competition and Data Privacy*, 12.

2.4 The Economic Value of Data Assets in Hotel Acquisitions

The economic theory of data valuation provides another crucial dimension for understanding disclosure limitations in hotel M&A transactions. As data has emerged as a strategic asset class, theoretical frameworks are essential for quantifying its economic value so that disclosure boundaries can be appropriately determined.

In the hotel industry, data analytics has become a critical tool for making informed decisions, identifying synergies, and maximizing the value of strategic transactions. This transformation positions data not merely as an operational tool but as a core asset driving acquisition value. Therefore, economic theory of data valuation must account for both historical performance metrics and predictive future value generated through analytics.[21]

Data's economic value in hotel acquisitions spans multiple dimensions. It provides critical insights for due diligence and accurate valuation of hotel properties, through the analysis of financial statements, occupancy rates, average daily rates (ADR), revenue per available room (RevPAR), and other key performance indicators.[22] Additionally, data facilitates the identification of synergies and integration opportunities; it enables guest experience optimization through the analysis of guest data and preferences.[23]

This multifaceted economic value presents a theoretical challenge for disclosure limitations. If data represents a significant portion of a target hotel's value, then restrictive disclosure could impede accurate valuation. However, if that same data includes protected personal information, then comprehensive disclosure might violate data protection principles. This tension demands theoretical frameworks for distinguishing between essential and non-essential data for transaction purposes.[24]

Economic theory also recognizes data's role in creating sustainable competitive advantage. The application of data-driven insights is instrumental in enabling stakeholders to make informed decisions, maintain a competitive edge in the market, and adapt to evolving customer preferences.[25] This forward-thinking value may be difficult to measure during the due diligence

[21] YANG, 2025.
[22] KIM, 2020.
[23] ARTEAGA & ROSSELLÓ, 2012.
[24] OECD, 2011. *Information Exchanges between Competitors under Competition Law.*
[25] KIM, 2020.

process, potentially requiring the provision of more extensive historical data to facilitate predictive modeling.[26]

Following the collection of pertinent information, the buyer is able to accurately assess the transaction. The disclosure of information during the pre-transaction phase is advantageous when considering economic factors and transaction decisions. Such transparency ensures a fair deal that aligns with the buyer's economic objectives.

Furthermore, the economic theory of hotel data valuation must acknowledge distinct data categories with varying economic utility and disclosure sensitivities. Guest preference data may offer significant operational insights without necessarily containing highly sensitive personal information, while payment data might present substantial compliance risks with limited incremental valuation insights.

2.5 Conflict Between Disclosure Needs and Data Protection Obligations

Theoretically, there is a tension between disclosure requirements in M&A transactions and data protection obligations. This tension represents a central challenge and requires careful theoretical analysis. This conflict is evident throughout the transaction process, from preliminary discussions through due diligence and into post-acquisition integration.

The fundamental reason for this theoretical conflict is that M&A transactions are "based on a demanding, challenging, and complex negotiation process, dynamic and phased over time, characterized by its uncertainty."[27] The pre-contractual phase is marked by an information asymmetry between the buyer and the seller. This creates a need for extensive disclosure to reduce uncertainty and allocate risk appropriately. However, data protection obligations may impose significant restrictions on such disclosure.[28]

The GDPR's impact on M&A disclosure is significant. Its substantial penalty risk creates strong incentives to limit data disclosure, which could potentially conflict with the thorough information exchange traditionally expected in M&A transactions[29].

One potential solution to this issue would be to implement structural limitations on data access. The data room concept serves as a primary mechanism for controlled disclosure, with

[26] PINHO, 2024.
[27] RAMA DOS SANTOS, 2024: 2.
[28] Ibidem.
[29] CMS LAW, 2020.

variations including standard data room protocols for hotels and the black box data room approach.[30] These structural limitations are designed to balance the buyer's legitimate need for information with legal restrictions on data transfers.

Another theoretical solution is phased disclosure strategies, which allow for gradually increasing access to sensitive information as the transaction progresses and additional safeguards are implemented.[31] This approach is consistent with the understanding that M&A negotiations are characterized by a demanding, challenging, and complex negotiation process that is dynamic and phased over time.

Furthermore, the theoretical framework must account for appropriate anonymization and redaction requirements as potential compromise solutions. By removing personal identifiers while preserving aggregated insights, these techniques may satisfy both disclosure needs and data protection obligations in certain contexts.[32]

To illustrate, in the event that a seller possesses 20,000 marketing emails and 3,800 loyalty program members, the value of the data remains anonymous and is not subject to data protection regulations. Consequently, the buyer could access the data without restrictions regarding direct data protection. The determination of whether to disclose information is a subjective matter that is contingent upon the parties involved. However, it can be argued that this decision is influenced by compliance measures.

It is also essential to distinguish between disclosure limitations arising from legal obligations and those stemming from commercial confidentiality concerns; this reflects a major difference. While both may restrict information sharing, they operate under different theoretical frameworks and may justify different types of disclosure limitations.

3 Regulatory Landscape Establishing Disclosure Limits

The hospitality industry functions within a multifaceted regulatory framework that establishes boundaries for information disclosure and data sharing. These regulations profoundly affect the operational protocols of hotels, particularly in cross-border contexts where multiple legal jurisdictions intersect. The increasing digitization of guest information and the global nature of

[30] KUMMER, 2007.
[31] CUNHA, 2016.
[32] STAM & KLEINER, 2020.

hotel chains necessitate an inmense understanding of these regulatory landscapes to ensure compliance, protect guest privacy, and facilitate legitimate business transactions.

This chapter examines the multifaceted regulatory environment that establishes disclosure limits in the hospitality industry. It focuses on Portugal and Spain's frameworks, industry-specific regulations, and the jurisdictional conflicts that emerge in cross-border hotel mergers and acquisitions.

The analysis indicates that while regulatory frameworks are designed to safeguard personal data, they also generate substantial compliance challenges for hotel operators engaged in international business activities.

3.1 European Union Framework: GDPR as a Limit to Information Exchange

The General Data Protection Regulation, which was implemented on May 25, 2018, is regarded as the most comprehensive data protection framework globally. It establishes significant limits on information exchange within the hospitality sector. This regulation fundamentally altered the manner in which hotels collect, process, store, and share personal data of European Union citizens, irrespective of the hotel's physical location. The GDPR predicated on several core principles that directly impact information exchange in the hospitality context. These core principles include purpose limitation, data minimization, and restrictions on cross-border data transfers[33].

The purpose limitation principle, delineated in Article 5(1)(b) of the GDPR, stipulates that personal data must be "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[34] For the hospitality industry, this signifies that guest data collected for the purpose of facilitating reservations cannot subsequently be utilized for unrelated marketing initiatives without a legitimate legal basis or explicit consent from the guest.

This principle imposes substantial restrictions on the free flow of information within hotel operations and between business partners, as each data transfer must be justified by the original purpose or obtain new consent. The regulation unequivocally prohibits the repurposing of data without appropriate justification; hotels are prohibited from disseminating guest data to external

[33] INFORMATION COMMISSIONER OFFICE (ICO), 2018. "Guide to the General Data Protection Regulation"
[34] GDPR (2016). Art 5(1)(b).

partners absent either an alignment with the original purpose or the satisfaction of additional stringent criteria.[35]

Moreover, the data minimization principle articulated in Article 5(1)(c) stipulates that personal data must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[36] In practical terms, this necessitates that hotels ascertain the minimum amount of personal data required to fulfill their operational purposes and prohibits the collection of excessive information.

It is important for hotels to regularly check their data processing operations to make sure they only keep information that is directly related to their business, and get rid of any extra data. This law restricts how much and what kind of information can be shared in the hospitality industry.

The GDPR establishes stringent criteria for the transfer of personal data beyond the European Economic Area (EEA), thereby imposing significant impediments to the exchange of information for international hotel chains. Article 44 of the GDPR delineates the criteria under which the transfer of personal data to a third country or international organization is permissible[37].

These criteria include the existence of adequacy decisions, the implementation of appropriate safeguards, or the receipt of explicit consent from the data subject[38]. These provisions directly impact cross-border hotel operations, necessitating the implementation of complex legal mechanisms to facilitate necessary data transfers while maintaining compliance.

Hotels are obligated to comply with these requirements when disseminating guest information across different jurisdictions or when employing global reservation systems and customer relationship management platforms.

3.2 Comparative Analysis of Regional Disclosure Limitations

3.2.1 Portugal's Approach to Data Disclosure Boundaries

Portugal has adopted a unique approach to data privacy through Law 58/2019 of August 8, which ensures the execution of the General Data Protection Regulation within the Portuguese jurisdiction while introducing additional national provisions[39]. The Portuguese legal framework

[35] ISSAOUI ET AL., 2023.
[36] GDPR (2016). Art 5(1)(c).
[37] GDPR. Article 44.
[38] OLDANI, 2020.
[39] PORTUGAL: Lei n.º 58/2019, de 8 de agosto.

incorporates a series of country-specific obligations that impose further restrictions on the disclosure of information within the hospitality sector.

Most notably, Portugal has established more stringent requirements concerning the processing of health and genetic data. The law mandates that entities access such data exclusively by electronic means, except where technically unfeasible or when the data subject explicitly requests otherwise.[40] Moreover, the law prohibits the subsequent transmission of health and genetic data, thereby creating a substantial impediment to the flow of information for hotels that may collect health-related information from guests for accommodation purposes or specialized services.[41]

The Portuguese regulatory framework imposes additional obligations on Data Protection Officers (DPOs) within the context of hotel operations. In addition to the requirements established by the GDPR, Portuguese law stipulates that DPOs must "ensure that both periodic and unscheduled audits are carried out" and “ensure that users are informed of the significance of promptly identifying security incidents and the imperative to notify the security officer without delay.”[42]

The growth of these responsibilities has led to the creation of stronger ways to oversee data processing activities in Portuguese hotels. These mechanisms effectively limit opportunistic or unplanned information disclosure through enhanced vigilance and accountability structures.

A distinguishing feature of Portugal's approach pertains to its enforcement mechanisms. The Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados or CNPD) has been explicitly appointed as the supervisory authority through Law 58/2019[43]. The CNPD wields considerable authority in the duty of monitoring compliance and the imposition of sanctions for violations; thereby offering a compelling incentive for hotels operating within Portugal to exercise stringent oversight with regard to information disclosure practices. However, it is noteworthy that the CNPD has issued Decision 494/2019, which states that specific provisions of Law 58/2019 will not be implemented due to their potential incompatibility with the GDPR.

According to Portuguese law, there are clear rules about collecting personal data from hotel guests for law enforcement purposes. According to the rules of the Convention Implementing the

[40] PORTUGAL: Decree-Law 80/2017. Article 26.
[41] Ibidem. Article 17.
[42] PORTUGAL: Lei n.º 58/2019, de 8 de agosto. Article 11. [Unofficial translation from original (Portuguese)].
[43] PORTUGAL: Lei n.º 58/2019, de 8 de agosto. Article 3.

Schengen Agreement, hotels and other places of hospitality have to collect certain personal information from guests and make this information available to the relevant authorities if it's needed to prevent a threat or to conduct a criminal investigation.[44]

However, when such personal data is communicated, Portuguese authorities must ensure a certain level of data protection in line with established principles, creating a balanced approach that allows necessary information sharing while maintaining appropriate safeguards.[45] This dual purpose framework engenders an environment in which hotels must concurrently fulfill their obligations to law enforcement and protect the privacy rights of their guests.

3.2.2 Spain's Limits on Information Sharing

Spain has implemented particularly stringent regulations on information sharing in the hospitality sector, establishing one of the most restrictive frameworks within the European Union. The implementation of Royal Decree 933/2021, effective from December 2, 2023, has dramatically expanded the data collection and reporting requirements for hotels, creating significant new disclosure obligations that restrict the free flow of information by channeling it through regulated pathways.[46]

According to the provisions of this decree, hotels operating within Spain are obligated to collect and submit an extensive array of personal data from guests, including payment details, residential addresses, telephone numbers, email addresses, and familial relationship information.[47] This information is to be submitted to the relevant Spanish security forces through a designated platform within 24 hours of collection. Failure to comply with this directive may result in financial penalties.

The recently implemented system necessitates that business entities register with the SES HOSPEDAJES platform, which has been in existence since 2022.[48] For tourists and residents of Spain, this entails furnishing additional personal information during their stay, including phone numbers, email addresses, and details regarding their travel companions. The hospitality industry is concerned about the potential repercussions on guest satisfaction. The implementation of these additional measures may result in prolonged wait times at check-in counters.

---

[44] GESLEY, 2019.
[45] CANTO MONIZ, 2020.
[46] SPAIN: Royal Decree 933/2021.
[47] Ibidem. Annex 1.
[48] KLEIDERMAN, 2024.

The Spanish Data Protection Agency (AEPD) has provided specific guidance on maximum storage periods through several consultation responses. In December 2020, the AEPD emphasized that storage periods must be determined based on the accountability principle, with the data controller bearing responsibility for establishing appropriate retention timeframes.[49]

The Spanish regulatory approach signifies a substantial departure from conventional data protection frameworks, as it stipulates extensive data sharing with governmental authorities while concurrently imposing restrictions on the utilization of this very information for other objectives.

Hotels are obligated to collect and report over 40 pieces of information for accommodation bookings, which significantly exceeds the data collection requirements in other European jurisdictions.[50] This results in a scenario where hotels are compelled to collect and disclose significant guest information to authorities; yet, they are subject to substantial restrictions on the utilization of this data for their own business purposes under GDPR provisions. The Spanish Confederation of Hotels and Tourist Accommodation (CEHAT) has articulated a pronounced disapproval of these stipulations, citing concerns regarding data aggregation, storage, privacy implications, and the possibility of operational burdens.[51]

Spain's regulatory framework has been the subject of scrutiny, as it has the potential to conflict with the broader European data protection principles that have been established. Critics contend that the comprehensive data collection mandated by Royal Decree 933/2021 may be excessive and disproportionate to the stated objectives of enhancing public safety and combating terrorism and organized crime[52].

The need to collect and retain sensitive information, such as credit card details, has raised specific concerns, as European data protection agencies generally prohibit such practices. These tensions highlight the complex relationship between national security interests and privacy protection, creating significant compliance challenges for hotels operating within Spain.

The implementation of these regulations has generated operational concerns within the Spanish hospitality industry, with fears of increased administrative burdens, longer check-in times, and potential damage to the guest experience. CEHAT has explored the legal recourse available to

[49] AEPD (SPAIN) - PS/00078/2021.
[50] KLEIDERMAN, 2024.
[51] SPAIN: Ministry of Interior. (2024). *Partes de Entrada.*
[52] MENENDEZ-ROCHE, 2024.

challenge the decree, citing a paucity of dialogue with the government and potential conflicts with the European Union's General Data Protection Regulation.[53]

This regulatory conflict shows the challenges that come up when national security goals meet international data protection rules. This creates a complicated compliance landscape for hotels operating in Spain and might affect how information flows between international hotel chains that have properties in the Spanish market.

3.2.3 International Frameworks Affecting Cross-Border Hotel Transactions

Cross-border hotel transactions operate within a complex landscape of international frameworks that establish varied disclosure limitations across jurisdictions. The Financial Stability Board (FSB) has identified the transfer of data across borders as being essential to the functioning of cross-border payment systems.

These systems are crucial for hotel transactions involving international guests or multinational operators. However, these data transfers are subject to a range of data frameworks that vary significantly between jurisdictions, creating friction in cross-border information exchanges[54]. These frameworks address a variety of aspects of data governance, including conditions for cross-border transfers, data storage requirements, security protocols, and technical standards that affect information sharing in hotel operations[55].

International hotel chains must navigate significant variations in data privacy approaches across regions. The European Union's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL) constitute distinct regulatory frameworks, each with its own distinct requirements for data collection, processing, and transfer[56].

These disparities engender compliance challenges for hotels with global footprints, as evidenced by a case adjudicated by the Guangzhou Internet Court[57]. The case involved an international hotel group accused of unlawfully transferring personal data to various overseas entities during a hotel reservation process. The court determined that while the transfer of data to

[53] Ibidem.
[54] FINANCIAL STABILITY BOARD (FSB), 2024. *"Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments"*
[55] FINANCIAL STABILITY BOARD (FSB), 2023. *"Stocktake of International Data Standards Relevant to Cross-Border Payments"*
[56] Ibidem.
[57] (2022) Yue 0192 Min Chu No. 6486

the hotel in Myanmar for reservation purposes and to an entity in France managing the central reservation system was lawful as necessary for contractual performance, the transfer of personal data to other overseas entities for marketing purposes without separate consent was unlawful[58]. This case exemplifies the intricate interpretations of necessity and consent that hotels must deliberate when disseminating information across international borders.

The regulatory environment for short-term accommodation rentals has become increasingly intricate following the implementation of the European Union Regulation on data collection and dissemination for short-term accommodation rentals, encompassing data-sharing provisions[59]. This regulatory framework stipulates that platforms must submit monthly reports to local authorities, encompassing details such as the rental's location, its classification, and the personal information of guests.

The regulation's objective is to harmonize and streamline the framework for data generation and sharing across the EU by establishing national "single digital entry points" for data transmission between online platforms and public authorities[60]. This results in the establishment of an additional layer of disclosure requirements that affect hotel operators engaged in short-term rental activities. Consequently, new pathways for mandatory information sharing are created while restricting other forms of data exchange.

International frameworks also address the technical aspects of data exchange in cross-border transactions. Numerous authorities have underscored the merits of interoperable data principles and standards, emphasizing their potential to enhance data portability and facilitate cross-border data flows[61].

The implementation of standardized messaging formats, notably ISO 20022, has been identified as a beneficial strategy for facilitating necessary information exchange while maintaining appropriate safeguards[62]. These technical standards aim to reduce payment rejections and allow for payment traceability, addressing some of the friction points in cross-border hotel transactions while operating within the boundaries established by data protection regulations[63].

---

[58] WEISS ET AL, 2024.
[59] COUNCIL OF THE EU TOURISM, 2024. *"Council gives its final approval to the regulation for short-term rentals".*
[60] Ibidem.
[61] CONSTANTINO ET AL, 2024.
[62] FINANCIAL STABILITY BOARD (FSB), 2023. "*Stocktake of International Data Standards Relevant to Cross-Border Payments",*
[63] BANK FÜR INTERNATIONALEN ZAHLUNGSAUSGLEICH, 2023.

3.3 Industry-Specific Regulations Affecting Hotel Data

Hotels are particularly vulnerable to data protection concerns as they handle vast amounts of personal information daily, including guest names, payment details, passport information, and sometimes sensitive data such as dietary preferences or health requirements[64]. This strategic positioning places hotels under the scrutiny of various data protection laws, necessitating specific industry adaptations to ensure compliance while maintaining operational efficiency.[65]

Industry-specific regulations often address the unique ways hotels collect and process guest data. Hotels obtain high volumes of personal data from multiple sources, including third-party booking systems, corporate websites, direct reservations, and walk-in guests. This multi-channel data acquisition process creates complex compliance requirements, as hotels must ensure appropriate data collection practices across all touchpoints [66]. The high rate of employee turnover and the use of independent contractors in the hotel industry further complicate data handling protocols, requiring robust training and governance structures to maintain compliance. Some hotels also operate CCTV systems and conduct customer profiling activities, which adds further layers of regulatory considerations specific to the hospitality context [67].

The hospitality industry has its own set of challenges when it comes to marketing and managing customer relationships. Hotels often use direct marketing, loyalty programs, and personalized service offerings that rely on guest data. Regulations establish specific boundaries for these activities. They require explicit consent for marketing communications and establish rules for the operation of loyalty programs. For example, hotels must get permission to send marketing messages, offers, or promotions, and they must let customers limit how their data is used for these purposes. These industry-specific uses of general regulatory ideas create a specialized compliance landscape that hotels must navigate to balance personalized service delivery with privacy protection.

The 2016 ruling in the Marriott-Starwood case is regarded as a seminal piece of legal doctrine, providing a foundational understanding of the risks and limitations of data privacy in the hospitality sector. The acquisition revealed systemic failures in Starwood's cybersecurity from

[64] CALIKOGLU ET AL, 2020.
[65] PANKAJ, 2025.
[66] AKKSHAY, 2024.
[67] AROKUN, 2025.

2014 onward, resulting in the compromise of personal data, including passport numbers and payment details, of approximately 500 million guests. Following the acquisition, Marriott was confronted with a substantial financial obligation, amounting to a fine of 99 million pounds and remediation costs that exceeded 700 million pounds. This case underscores the necessity of pre-merger and acquisition audits of information technology systems and the appropriate service level agreements to avert data breaches.[68]

Industry associations have created special instructions to help hotels put in place the right technical and organizational steps. These instructions are based on the specific way hospitality businesses operate. This includes recommendations for handling a high number of payment card transactions, managing long-term data storage, and implementing appropriate data security measures across multiple customer touchpoints.

3.4 Jurisdictional Conflicts in Cross-Border Hotel M&A

Cross-border mergers and acquisitions in the hotel industry present distinctive jurisdictional challenges related to data disclosure and regulatory compliance. Given the international nature of many hotel operations, M&A transactions frequently involve the transfer of substantial amounts of personal data across different legal jurisdictions, each with its own regulatory framework.[69]

These jurisdictional variations introduce significant complications in the processes of mergers and acquisitions due diligence, transaction structuring, and post-acquisition integration. The acquiring company must assess and mitigate the risks associated with differing data protection regimes. The disparities in regulatory frameworks across jurisdictions engender an inequitable environment, wherein businesses encounter divergent levels of compliance obligations and legal ambiguity contingent on the involved territories within a transaction.[70]

In the context of cross-border hotel M&A, due diligence processes must address the target company's compliance with multiple data protection regimes. Conducting thorough due diligence is critical in any M&A transaction, but it becomes even more crucial in a cross-border context, where different legal systems, business practices, and cultural nuances intersect [71].

[68] FEDERAL TRADE COMMISSION, 2024.
[69] HALL, AARON. *"Legal Challenges in Cross-Border Mergers and Acquisitions".*
[70] HANSSON, 2024.
[71] AROKUN, 2025.

A comprehensive legal due diligence evaluation encompasses a meticulous assessment of the target's contractual agreements, historical litigation records, adherence to local data protection legislation, and intellectual property rights pertaining to customer data and hotel management systems. A particularly salient case that exemplifies these risks involved a global hotel chain in Turkey. In this instance, the Turkish Constitutional Court adjudicated a case concerning administrative fines imposed by the Data Protection Authority for a data breach affecting 500 million customers' personal data[72]. The hotel chain contested the fine, arguing that the breaches occurred before its acquisition of the company and during the previous owner's tenure[73].

Following the completion of a merger or acquisition, the integration process is complicated by the need to maintain compliance with multiple regulatory frameworks simultaneously, particularly when the transaction involves properties or operations in different jurisdictions[74]. These determinations have a substantial impact on the manner in which guest data can be collected, processed, and shared across the newly integrated organization.

In the context of mergers and acquisitions deals, common transfer safeguard options include adequacy decisions recognizing equivalent protection in the destination country or the implementation of Standard Contractual Clauses (SCCs) between the entities involved. These requirements introduce a degree of complexity to the processes of deal structuring and execution, with the potential to affect both transaction timelines and the planning of integrations.[75]

Given the complexity and scope of privacy laws applicable to hotels, proprietors must meticulously tailor covenants and indemnities to explicitly delineate risk allocation between the parties. Furthermore, an increasing number of parties to hotel management agreements are incorporating provisions for adequate cyber liability insurance. This insurance provides coverage for a wide range of potential costs associated with data breaches, extending beyond direct financial losses. These costs may include legal fees, regulatory fines, guest compensation, and expenses related to reputational management[76].

[72] CONSTITUTIONAL COURT OF TURKEY (2020/7518).
[73] YURTSEVER, 2024.
[74] CALIKOGLU ET AL, 2020.
[75] ILAN ET AL, 2016.
[76] TENE ET AL, 2024.

3.5 Summary of the Chapter

The regulatory framework that establishes disclosure limits in the hospitality industry is multifaceted, significantly impacting information exchange in hotel operations and cross-border transactions. GDPR serves as a foundational pillar, establishing comprehensive principles that restrict how personal data can be collected, processed, and shared within the hospitality context. Regional variations, as evidenced by Portugal's additional requirements for health data and Spain's extensive data collection mandates for security purposes, further complicate compliance efforts for international hotel operators. The use of different regulatory methods creates a complicated environment, which forces hotels to follow many different rules about information disclosure at the same time. These rules can sometimes be inconsistent.

The unique characteristics of the hospitality sector requires the adaptation of broader data protection principles to meet specific industry needs. It is the responsibility of hotels to implement effective governance frameworks that address these unique operational features while maintaining compliance with applicable regulations. The challenges associated with cross-border M&A transactions are particularly noticeable because of differences in regulations between countries. These conflicts can make it hard to do the necessary research, transaction structuring, and post-acquisition integration.

The evolving nature of data protection regulations, evidenced by recent developments such as Spain's Royal Decree 933/2021 and the EU Regulation on short-term accommodation rentals, suggests that the regulatory landscape will continue to shift, requiring ongoing adaptation by hotel operators.

It is imperative that future research explore emerging regulatory trends, particularly concerning the development of international frameworks that may harmonize data protection approaches across jurisdictions. Furthermore, additional investigation into effective compliance strategies for multinational hotel chains operating across diverse regulatory environments would provide valuable insights for industry practitioners navigating this complex topic.

4 Pre-Contractual Data Disclosure Duties and Limits

It is important to understand that pre-contractual transactions create different concerns about guest data, loyalty program information, and proprietary operational systems that may not be

present in other industries. The hospitality sector relies on personal data, which creates challenges during the due diligence process. This is because the sector must balance transparency and the legal protection of sensitive information.

From a theoretical perspective, the disclosure of information in M&A transactions serves to reduce the information gap between the parties involved in the transaction. However, it should be noted that this disclosure obligation is not absolute. While these measures have the potential to mitigate information asymmetry in specific domains, they may also impede the generation of private information and reduce opportunities for risk-sharing.[77] This theoretical tension serves as the foundation for the legal frameworks governing disclosure obligations across different legal jurisdictions.

The European regulatory landscape regarding disclosure obligations in M&A transactions reflects this tension, with varying approaches across member states despite efforts toward harmonization.[78] The considerable variation in disclosure requirements across EU member states gives rise to regulatory challenges for cross-border transactions, particularly in sectors such as hospitality, where operations frequently extend across multiple jurisdictions.

According to Portuguese legislation, there is no general statutory duty of information explicitly imposed upon sellers in M&A transactions. However, Portuguese legal doctrine has evolved to adopt a more nuanced approach through the interpretation of the Civil Code. Specifically, Articles 227 and 762, paragraph 2 of the Portuguese Civil Code have been interpreted to establish that "sellers should act in good faith prior to the conclusion of the transaction and certain information should be disclosed."[79]

Portuguese jurisprudence further stipulates that all information disclosed must be "correct, clear, and true; otherwise, sellers may ultimately be held liable for damages."[80] The scope of this disclosure obligation is determined by various factors, including the specific contract to be concluded, the target's structure and activity, and other considerations, such as its risk. In practice, this necessitates that sellers disclose any impediments that could impede transaction completion,

[77] GENCHEVA & DAVIDAVIČIENĖ, 2016.
[78] RIMARCHI & STROPPA, 2020: 39.
[79] BATISTA ET AL, 2024.
[80] Ibidem.

circumstances that could affect long-term profitability, or any other information deemed essential to the buyer's acquisition decision.[81]

In the context of transactions involving public companies in Portugal, there exists a particular set of additional disclosure requirements that must be observed. The Portuguese Securities Code stipulates that "information concerning a prospective deal must be immediately disclosed as soon as the target company becomes aware of the commencement of any negotiations or their likely commencement."[82] However, disclosure may be temporarily withheld if its release could potentially hinder legitimate interests or mislead investors, provided that confidentiality is maintained.

The Spanish legal system imposes more explicit obligations regarding pre-contractual disclosure in mergers and acquisitions transactions. Even in the absence of formal preliminary agreements, Spanish law establishes that "the parties have the obligation to negotiate in conformity with fair and honest conduct, and to act with loyalty."[83] This fundamental principle of good faith in pre-contractual negotiations establishes a fundamental duty of information disclosure.

The regulatory framework governing M&A transactions in Spain includes several key legislative instruments that influence disclosure obligations. The Spanish Companies Act (Ley de Sociedades de Capital) establishes the overarching corporate governance framework, while the Securities Market Act (Ley del Mercado de Valores) stipulates specific disclosure requirements for transactions involving public companies.[84] Additionally, the Takeover Law (Ley de Opas) governs public tender offers and mandates detailed disclosure to ensure transparency in transactions.[85]

Spanish judicial precedent has established that disclosure obligations extend beyond formal reporting requirements to include substantive good faith in information sharing. This principle aligns with the broader tenet that M&A transactions should be fair, transparent and in a way that protects shareholder interests and market integrity.[86]

Recent European jurisprudence has further clarified the standards for adequate disclosure in M&A transactions. The German Federal Court of Justice (BGH) established a significant precedent

[81] DLA PIPER, 2024.
[82] ABREU ET AL, 2024.
[83] SÁNCHEZ & NOGUER, 2020.
[84] LAWANTS, 2025.
[85] LAWANTS, 2025.
[86] Ibidem.

in its September 15, 2023 ruling,[87] determining that the mere uploading of documents to a data room does not suffice to satisfy disclosure obligations. The court delineated two conditions that must be fulfilled for adequate disclosure: first, the buyer must have an actual opportunity to access the relevant information in the data room; second, the seller must reasonably expect that the buyer would discover material information through data room inspection.[88]

The BGH has determined that sellers must explicitly disclose such information to buyers, particularly when it is not readily apparent from data room documents. This requirement is deemed to be of very considerable economic importance.[89] This ruling signifies a substantial progression in European M&A jurisprudence, with the potential to influence Spanish and Portuguese practices as they are fellow EU member states, despite the lack of direct binding effect across jurisdictions.

4.1 Legitimate Boundaries of Pre-Contractual Information Sharing

During the pre-contractual phase, substantial information exchange is essential; however, this exchange must adhere to established guidelines. These guidelines are defined by competition law, privacy regulations, and contractual provisions, ensuring that the exchange of information occurs within appropriate boundaries.

Non-disclosure agreements (NDAs) are the primary contractual mechanism for establishing these boundaries.[90] In the hotel industry, NDAs must address both the typical concerns found in any M&A transaction and the specific sensitivities of the hospitality sector. When negotiating NDAs for hotel acquisitions, parties must consider the confidential information,[91] potential recipients or parties and exceptions to these obligations.

When potential buyers and sellers are competitors, it is essential to exercise additional caution to prevent any potential violations of competition law. As CMS Law states: "There is a general business need to share information with potential purchasers in the context of an M&A deal […] [However,] special caution should be exercised if the potential seller or purchaser are competitors or have market overlap, in order to mitigate competition law risks."[92] This

[87] FEDERAL COURT OF JUSTICE, September 15, 2023 - V ZR 77/22.
[88] KPMG LAW, 2023.
[89] MORGAN LEWIS, 2023,
[90] MORGAN LEWIS, 2020.
[91] In the context of hotel transactions, this definition should explicitly address guest data, loyalty program information, vendor relationships, and proprietary operational systems.
[92] CMS LAW, 2019.

phenomenon is especially relevant in the hotel industry, where geographic competition and market segmentation frequently result in competitive overlaps between transaction parties. In the hospitality sector, competitive information such as room rates, occupancy levels, and customer acquisition costs requires particular protection.[93]

4.2 Justified Refusal of Information Sharing

While comprehensive disclosure remains a cornerstone of M&A transactions, both Spanish and Portuguese legal frameworks recognize circumstances where sellers can legitimately refuse to share certain information during pre-contractual negotiations.[94]

In the context of the Spanish hotel sector, this categorization would encompass detailed data on pricing strategies for specific market segments, customer acquisition costs, and strategic expansion plans for competitive geographic markets.[95]

The Portuguese Securities Code explicitly reinforces this principle in the article 12-C and 248-A by allowing companies to "withhold disclosure for the period required to complete the relevant negotiations, as long as it ensures the confidentiality of such information".[96] This provision establishes a legal basis for the withholding of information during the negotiation phase of hotel acquisitions, particularly when disclosure could potentially compromise the competitive positioning of the relevant parties.

The legal systems of Spain and Portugal acknowledge the obligatory nature of confidentiality provisions in third-party agreements. The Spanish General Court's jurisprudence has established that contractual confidentiality obligations remain enforceable even during M&A processes, creating legitimate grounds for refusal to share information subject to such restrictions.[97] In the context of the hotel industry, this matter assumes particular pertinence with regard to franchise agreements, management contracts, and technology licensing arrangements, which frequently encompass comprehensive confidentiality provisions.

This graduated approach to information sharing holds particular value in the context of hotel industry transactions, where concerns regarding competition, data protection obligations, and

[93] MINTZ ET AL, 2022.
[94] PÉREZ-ORDÓNEZ, 2021: 141.
[95] CLAVER ET AL, 2006.
[96] COMISSAO DO MERCADO DE VALORES MOBILIARIOS. Security Code. Last reform of 2015.
[97] CHRISTOPHER THOMAS AND GIANNI DE STEFANO, 2016.

contractual restrictions frequently intersect. The implementation of a structured disclosure program, one that respects legal boundaries while facilitating necessary due diligence, enables transaction parties to navigate the complex legal landscape governing information sharing in Iberian hotel M&A transactions.

4.3 Summary of the Chapter

The limits of data disclosure in hotel industry M&A transactions are defined by a careful balance between the need for transparency and the protection of sensitive interests. Theoretical and legal frameworks in both Portugal and Spain emphasize the reduction of information asymmetry through good faith disclosure, yet these obligations are not absolute.

Sellers must ensure that information provided is correct, clear, and sufficient for informed decision-making, but may withhold competitively sensitive data, personal information protected by law, or details restricted by contractual agreements. European jurisprudence, such as the German Federal Court of Justice's recent guidance, further clarifies that disclosure must be effective and targeted, especially for information of significant economic importance, and not merely a formal exercise. In practice, the hospitality sector's reliance on guest data, proprietary systems, and complex contractual relationships necessitates a nuanced, phased approach to information sharing, guided by non-disclosure agreements and regulatory standards.

The rules about sharing data when a hotel company joins with another company are determined by several factors, including trust, competition laws, data protection, and contracts. Sellers must understand these limits to make sure that the process of selling their company is both fair and correct.

5 Categories of Protected Hotel Data and Their Disclosure Thresholds

In the contemporary hospitality industry, hotels serve as substantial repositories of diverse personal and commercial data, collected through numerous touchpoints across the guest journey. The digital transformation of hotel operations has resulted in a substantial increase in the volume and sensitivity of the data processed.

This has caused a shift in data protection from being a minor concern to a central operational and strategic imperative. This chapter provides a comprehensive examination of the various

categories of protected hotel data and analyzes the corresponding disclosure thresholds that define appropriate data handling practices within the hospitality industry.

5.1 Guest Personal Data

A guest's personal data encompasses a broad range of information that is commonly collected during the hospitality service cycle. Hotels collect and process significant amounts of personal data, including guests' names, contact information, payment details, identification documents, travel history, service preferences, and in some cases, biometric data and health information.[98]

Research for software usage purposes, has highlighted the complexities inherent in managing guest data transfers: "The most severe problems stem from data breaches, where the information is stolen as a consequence of compromised security, or is sold purposefully for monetary gain. In either scenario, personal information could end up in the possession of entities that the user did not intend to share it with."[99] This underscores the critical importance of establishing clear boundaries for the legitimate transfer of guest personal data, ensuring that such transfers occur only under properly defined and controlled circumstances. Currently, there are no regulations that specifically address taxative limitations or boundaries. However, the constant regulations and laws require a duty of care for this information, ensuring that it is protected and maintained in accordance with legal limits of the area of the subject.

5.1.1 Loyalty Program Data Disclosure Restrictions

Loyalty program data represents a particularly valuable subset of guest personal data. This data includes not only basic identification and contact information but also detailed behavioral patterns, preferences, spending habits, and cross-property stay history. This rich dataset, which enables personalized marketing and service delivery, is subject to specific disclosure restrictions due to its commercial sensitivity and privacy implications.[100]

Recent research on data vulnerability in hospitality contexts has established that loyalty program data requires enhanced protection due to its comprehensive nature and long-term retention periods. A 2024 study published in the Journal of Travel and Tourism Marketing found

[98] BRYNE, PAUL. *"How does GDPR apply to hotels?"*
[99] TOTH, 2022.
[100] LYNN, 2023: 33.

that "data privacy reduces data breach and access vulnerability, which increases privacy concerns, emotional violation, and switching intention."[101] This underscores the direct correlation between loyalty data protection and business outcomes, emphasizing the importance of strict disclosure restrictions.

From a regulatory perspective, the disclosure of loyalty program data is restricted by the principle of purpose limitation enshrined in most data protection frameworks. The GDPR stipulates that data should only be "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes"[102]. Consequently, data collected for the purpose of administering a loyalty program cannot be legitimately disclosed for unrelated purposes without additional legal bases or consent.

5.1.2 Payment Information Protection Requirements

Hotel payment information includes credit card details, bank account information, digital wallet data, and transaction records. The protection requirements for such financial data are particularly stringent, given the potential for direct financial harm resulting from unauthorized disclosure or access.[103]

The primary framework governing payment information protection in the hospitality industry is the Payment Card Industry Data Security Standard (PCI DSS), which establishes comprehensive requirements for the secure handling of cardholder data.[104]

A hotel's security protocol must encompass a rigorous set of measures to ensure the protection of guest payment data from potential misuse or alteration. These measures generally include data encryption, access controls, network segmentation, and regular security assessments. Implementing these measures is not just a matter of regulatory compliance.[105] Payment data breaches can result in substantial financial penalties, remediation costs, and reputational damage.

Research has demonstrated that consumers have significant concerns about payment data security in hospitality contexts. A recent study found that privacy concerns regarding payment information are a primary driver of customer anxiety and switching behavior.[106] This underscores

[101] YU ET AL., 2022: 215-227.
[102] GDPR (2016). Art. 5-6.
[103] PANKAJ, 2025.
[104] Ibidem.
[105] ROTH ET AL., 2020.
[106] YU ET AL., 2022: 215-227.

the need for hotels to not only meet minimum compliance requirements but also to adopt best protection measures that can be transparently communicated to guests to build trust.

In the rapidly evolving hospitality technology landscape, requirements for protecting payment information are also evolving. The increasing use of contactless payments, mobile payment applications, and tokenization technologies creates both challenges and opportunities for improving payment data security while reducing friction in the guest experience.[107]

5.1.3 Special Categories of Guest Data (Health, Biometrics)

In the context of hospitality, health data may encompass dietary restrictions, disability accommodations, medical conditions necessitating special arrangements, or health emergencies occurring on property. The scope of health data collected by hotels has expanded substantially due to the impact of the pandemic. Many properties have implemented measures such as temperature screening, vaccination verification, and contact tracing. The disclosure thresholds for such health data are exceptionally high, generally requiring explicit consent from the guest or a clear legal obligation (such as public health reporting requirements during disease outbreaks).[108]

Biometric authentication[109] offer an additional layer of security for system access. However, the disclosure thresholds for biometric data are particularly restrictive, with many jurisdictions requiring explicit, specific consent and prohibiting most forms of transfer or secondary use[110].

The management of special categories of guest data is further complicated by the varying international standards that exist. While the GDPR provides clear guidance on the handling of special category data in Europe, hotels operating globally must navigate a complex patchwork of regulations with differing requirements and disclosure thresholds.[111] This requires sophisticated data management systems capable of applying appropriate protection measures based on the data type.

[107] SALAMANCA, 2023.Antonio (2023). “Blockchain in the hospitality industry: Identifying main applications”.
[108] PILLAI ET AL., 2021.
[109] Usually, noted as fingerprint, iris scanning, facial recognition.
[110] LIYANAARACHCHI ET AL., 2023.
[111] RAMIC, 2022.

5.2 Employee Information: Transferability Limitations

Employee information in hospitality contexts encompasses a broad range of data types. These include personal identification details, employment history, performance evaluations, payroll information, scheduling preferences, and in some cases, health and biometric data used for time tracking or secure access.[112] The transferability of such information is subject to specific limitations arising from both data protection regulations and employment law.

The transferability limitations for employee information are particularly relevant in the context of HMAs between property owners and operators. As stated in the legal analysis, "Hotel owners seeking to protect themselves from privacy law violations and data breaches may consider incorporating clear covenants that require the operator to take certain measures to comply with privacy laws, protect guest data, and respond to any data breaches"[113]. The same considerations apply to employee data. HMAs are increasingly including explicit provisions that govern the handling and transfer of employee information during and after the term of the agreement.

Under the GDPR, employee data is subject to the same fundamental protections as other personal data. However, there are additional considerations that arise from the inherent power imbalance in the employer-employee relationship.[114] This raises concerns regarding the validity of consent as a legal basis for processing, as regulatory authorities generally recommend that employers rely on alternative legal bases such as contractual necessity or legitimate interests where possible[115]. These limitations on the legal basis for processing directly impact the transferability of employee information, restricting the circumstances under which such data can be legitimately transferred to third parties.

5.3 Trade Secrets & Necessary Disclosure

The hospitality industry generates substantial commercial data that requires protection. This data includes pricing strategies, occupancy rates, revenue management algorithms, customer acquisition costs, and market segmentation analyses. This commercial data often constitutes trade

[112] KUNER ET AL., 2020.
[113] TENE ET AL., 2024.
[114] BYGRAVE, 2017.
[115] LYNN, 2023.

secrets that provide a competitive advantage and thus warrant robust protection against unauthorized disclosure.[116]

The tension between protecting trade secrets and meeting necessary disclosure requirements creates complex challenges for hotel data management. As stated in a legal analysis, "The classification of these roles is fact-specific. It is essential for hotel owners and operators to carefully assess their roles to determine their legal designations under applicable privacy laws and to draft appropriate provisions to allocate privacy risks in an HMA."[117] This observation, while focused on personal data, applies equally to commercial data, where clear allocation of data ownership and disclosure rights is essential.

Hotels must develop nuanced policies that balance trade secret protection with necessary disclosure obligations. These policies should implement technical and organizational measures to ensure that disclosure is limited to what is strictly required by the specific circumstances.

Given the highly competitive nature of the hospitality industry, the protection of trade secrets is of paramount importance. Hotels invest significantly in proprietary revenue management systems, marketing strategies, and operational procedures that provide market differentiation. Unauthorized disclosure of this information could compromise our competitive advantage and result in significant business harm.[118] Consequently, hotels typically implement multi-layered protection measures for commercial data, including technical safeguards, contractual protections (such as NDAs), and clear internal policies governing data access and handling.

The evolution of data sharing in the hospitality ecosystem presents additional challenges for commercial data protection. As hotels increasingly participate in data-sharing initiatives to enhance industry benchmarking and market intelligence, they must carefully assess the balance between contributing to collective knowledge and protecting proprietary insights. This necessitates the implementation of advanced data anonymization techniques and the establishment of clear contractual frameworks that govern the use and further disclosure of shared commercial information[119].

[116] WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). *What is a Trade Secret?*.
[117] TENE ET AL., 2024.
[118] VOIGT & VON DEM BUSSCHE, 2017.
[119] BUHALIS & LEUNG, 2018.

5.4 Essential & Non-Essential Data

It is essential to distinguish between essential and non-essential data when implementing the data minimization principle that forms the foundation of modern data protection frameworks. In the hospitality industry, essential data refers to information that is strictly necessary to complete a specific transaction or deliver a requested service. Non-essential data encompasses supplementary information that may enhance the service experience but is not required for basic functionality.

The categorization of data as essential or non-essential has significant implications for consent requirements and disclosure thresholds. According to Article 6(1)(b) of the GDPR, the processing of essential data can often be justified based on contractual necessity; thus, allows for the processing of non-essential data, provided that explicit consent is obtained from the data subject.[120] This distinction establishes different disclosure thresholds, with essential data subject to relatively lower thresholds for legitimate processing and transfer within the boundaries of the primary service provision.[121]

The distinction between essential and non-essential data is not fixed; it changes in response to technological advancements, guest expectations, and regulatory interpretations. Hotels must regularly reassess their data collection practices to ensure alignment with current standards and implement appropriate technical and organizational measures that enable differentiated handling of data based on its classification.

5.5 Summary of the Chapter

The categorization of protected hotel data and the establishment of appropriate disclosure thresholds represent fundamental challenges in modern hospitality data management. As discussed in this chapter, hotels must deal with a variety of regulatory requirements, operational needs, and changing guest expectations regarding privacy and data protection.

An analysis of guest personal data, loyalty program information, payment details, and special categories of data has revealed the intricate nature of personal information in hospitality contexts and the varying levels of protection necessary. Likewise, the examination of employee

[120] GDPR (2016). ART 6(1)(B).
[121] INFORMATION COMMISSIONER OFFICE (ICO), 2018. "*Guide to the General Data Protection Regulation (GDPR)"*

information, commercial data, and the essential or non-essential distinction has underscored the necessity for nuanced approaches to data classification and protection.

An effective management strategy for protected hotel data necessitates an integrated approach that incorporates legal compliance, technical safeguards, organizational policies, and staff training. It is imperative that hotel staff is aware of how to collect, access, use, and disclose personal information, as well as how to restrict access to cardholder data.

6 Conclusion

6.1 Findings

The examination of data disclosure limitations in hotel industry mergers and acquisitions reveals a complex interplay between competing legal, economic, and operational imperatives. This research has comprehensively analyzed the theoretical foundations, regulatory frameworks, and practical implementations of data protection boundaries within hospitality sector transactions. The research focuses particularly on the European context, with emphasis on Portugal and Spain.

The fundamental tension that characterizes the disclosure of data concerning hotel mergers and acquisitions lies in balancing two legitimate but potentially conflicting interests. On the one hand, there is the buyer's need for comprehensive information to accurately assess value and risks. On the other hand, there is the legal obligation to protect sensitive personal and commercial guest data. The findings of this research demonstrate that this balance is not merely a practical challenge but is rooted in theoretical conceptions of data protection as a fundamental right and privacy as a non-price competition parameter.

The distinctive attributes of the hospitality industry serve to accentuate these tensions. Hotels serve as substantial repositories of diverse personal and commercial data, amassed through numerous interaction points throughout the guest journey. The digitalization of hotel operations has led to a substantial increase in the volume and sensitivity of processed data. This transformation has resulted in data protection becoming a central operational and strategic imperative.

The research has identified a multifaceted regulatory landscape that establishes disclosure limits in hotel M&A transactions. The General Data Protection Regulation serves as the foundational framework, establishing substantial restrictions through its core principles of purpose

limitation, data minimization, and cross-border transfer controls. These principles fundamentally alter how hotels can collect, process, store, and share personal data during transaction processes.

The presence of regional variations introduces further layers of complexity. For instance, Portugal's Law 58/2019 has instituted more stringent requirements for the collection and management of health and genetic data. In contrast, Spain's Royal Decree 933/2021 has led to a substantial expansion in the scope of mandatory data collection and reporting obligations. These national implementations engender a challenging compliance environment for international hotel chains engaged in cross-border transactions, requiring sophisticated data management strategies and legal expertise to navigate successfully. Further investigations are necessary to ascertain the true purpose of the royal decree, as it contravenes various limitations stipulated by the GDPR. This discrepancy has the potential to impact the outcomes of the mergers and acquisitions due diligence process.

In the context of hospitality, it is imperative to delineate that:

1. The collection and use of guest personal data, including information related to loyalty programs, is subject to the principles of purpose limitation. This data, which encompasses detailed behavioral insights and specific preferences, is subject to these principles to ensure the integrity of personal information and maintain the privacy of individuals.
2. Payment information is subject to PCI DSS requirements and heightened security protocols with the objective of preventing financial harm.

   With the same purpose, ISO 20022 measures apply security tools for handling information during internal or external usage.
3. A particular category of data, including health information and biometric data, necessitates explicit consent or a clear legal obligation for legitimate disclosure.
4. The transferability of employee information is subject to limitations that are specific to the context of data protection regulations and employment law considerations.
5. The establishment of commercial agreements necessitates a delicate balance between the protection of trade secrets and the imperative for disclosure in the context of relevant legal obligations.

The research has established that disclosure limits vary significantly across these categories, requiring nuanced approaches to data classification and protection throughout the M&A process.

The findings of this study demonstrate that effective implementation of disclosure limitations in the context of hotel M&A requires a structured approach that respects legal boundaries while facilitating the requisite due diligence.

6.2 Best Practice Advice

In order to ensure that mergers and acquisitions transactions are executed in accordance with the principles of fair trade, it is essential to devise and implement solutions designed to enhance best practices in these transactions. The following measures are of particular practical importance:

- Non-disclosure agreements serve as the primary contractual mechanism for establishing appropriate boundaries; it prevents breach of data by applying provisions addressing the hospitality data sensivity and its protection needs.
- The implementation of data room protocols, which are a series of guidelines that establish controlled disclosure environments, will encompass a range of approaches. These approaches will include standard protocols for hotels and black box methods for highly sensitive information.
- A recommended course of action is the implementation of a phased disclosure strategy. This entails the gradual augmentation of access to sensitive information as transactions proceed. It is also accompanied by the execution of additional safeguards.
- A crucial aspect for the sector is the need for anonymization and redaction requirements, as compromise solutions are contingent on the removal of personal identifiers while preserving aggregated insights. Therefore, the inclusion of analytics and anonymous statistics in the pre-transaction will facilitate the selection process for buyers. At the same time, sellers will be able to safeguard the data.

The limits of data disclosure in hotel M&A transactions reflect a delicate balance between facilitating informed business decisions and protecting fundamental rights and competitive interests. By following the recommendations above, M&A transactions can be conducted successfully by protecting data while allowing the transaction to progress.

7 References

ABREU ADVOGADOS: BATISTA, Santos, Marques & Carvalho
(2024), The Legal 500: Portugal, M&A, Abreu Advogados, Available in https://abreuadvogados.com/wp-content/uploads/2024/04/Legal-500-MA-2024.pdf

ABREU, Bernardo / OLIVEIRA, David / GALVAO, Joao
(2024), Corporate M&A, Available in https://practiceguides.chambers.com/practice-guides/corporate-ma-2024/portugal

AEPD (Spain)
(2021), PS/00078/2021, Available in https://gdprhub.eu/AEPD_(Spain)_-_PS/00078/2021

ALAN BUTLER and ENID ZHOU
(2021), Disease and Data in Society: How the Pandemic Expanded Data Collection and Surveillance Systems, American University Law Review, Available in https://digitalcommons.wcl.american.edu/aulr/vol70/iss5/2

ANNA GARDELLA, Massimiliano Rimarchi and Davide Stroppa
(2020), Potential Regulatory Obstacles to Crossborder Mergers and Acquisitions in the EU Banking Sector, EBA STAFF PAPER SERIES, Available in https://www.eba.europa.eu/sites/default/files/document_library/844126/Potential%20obstacles%20M&A.pdf

AROKUN, Esther
(2025), Addressing Privacy Risk Management in Mergers and Acquisitions: Developing a Compliance Strategy for Handling Third-Party Vendor Data, SSRN, Available in https://doi.org/10.2139/ssrn.5183834

ARTEAGA, Laura & ROSSELLÓ, Juana
(2012), The Impact Of Mergers And Acquisitions On Brand Value In The Hotel Sector During The Economic Crisis In Spain. A Case Study Of Nh Hoteles & Hesperia, Halmstad University Reproservice, Available in https://www.diva-portal.org/smash/get/diva2:538335/FULLTEXT01.pdf

BANK FÜR INTERNATIONALEN ZAHLUNGSAUSGLEICH
(2023), ISO 20022 Harmonisation Requirements for Enhancing Cross-Border Payments: Consultative Report, CPMI Papers 215, Bank for International Settlements

BRYNE, Paul
(2025), How does GDPR apply to hotels?, Available in https://propelfwd.com/how-does-gdpr-apply-to-hotels/

BUHALIS, Dimitrios, and LEUNG, Rosanna
(2018), Smart Hospitality-Interconnectivity and Interoperability towards an Ecosystem, International Journal of Hospitality Management, Available in https://doi.org/10.1016/j.ijhm.2017.11.011

BYGRAVE, Lee A.
(2017), Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, Oslo Law Review, Available in https://ssrn.com/abstract=3035164

CALIKOGLU, Melih / BURAH, Sel
(2020), GDPR Awareness and Compliance in the Hospitality Sector, Gasca Project Report, Available in https://www.academia.edu/119159871/GDPR_AWARENESS_and_COMPLIANCE_In_the_Hospitality_Sector_EN_TR_DE_

CANTO MONIZ, Graça
(2020), Is There Anything Left of the Portuguese Law Implementing the GDPR?: The Decision of the Portuguese Supervisory Authority, Personal Data Protection and Legal Developments in the European Union, Available in https://ssrn.com/abstract=4230775

Charter of Fundamental Rights of the European Union
(2000), Article 8, Available in https://www.europarl.europa.eu/charter/pdf/text_en.pdf

CHRISTOPHER THOMAS and GIANNI DE STEFANO
(2016), Non-compete clauses in M&A transactions: the EU Telefónica/Portugal Telecom judgments and some best practices.

CLAVER, Enrique, Rosario Andreu, and Diego Quer
(2006), Growth Strategies in the Spanish Hotel Sector: Determining Factors, International Journal of Contemporary Hospitality Management, Available in https://doi.org/10.1108/09596110610658607

CMS LAW
(2020), Checklist M&A and GDPR, CMS Hasche Sigle

CMS LAW
(2019), Information sharing concerns in transactions, Available in https://cms.law/content/download/377778/file/Information%20on%20sharing%20concerns%20in%20transactions%20-%20%20CEE.pdf

COMISSAO DO MERCADO DE VALORES MOBILIARIOS
(n.d.), Security Code, Available in https://www.edp.com/sites/default/files/securitiescodecons210920161.pdf

CONSTANTINO, João, Henrique São Mamede, and Miguel Mira Da Silva
(2024), Adopting ISO 20022: Opportunities, Challenges, and Success Factors for Corporations in Payment Processing, Emerging Science Journal, Available in https://doi.org/10.28991/ESJ-2024-08-04-010

Constitutional Court of Turkey
(2020), (2020/7518), Available in published in the Official Gazette on 15.12.2023

COUNCIL OF THE EU
(2024), Council gives its final approval to the regulation for short-term rentals, Press Release.

CUNHA, Juliana Bonazza Teixeira da
(2016), A Qualificadora "No Melhor Conhecimento" em Contratos de Compra e Venda de Participação Societária – Sao Paulo.

Directive 95/46/EC of the European Parliament and of the Council
(1995), on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

DLA PIPER
(2024), Data Protection in Portugal, Available in
https://www.dlapiperdataprotection.com/index.html?t=law&c=PT

DOBRINA GENCHEVA & VIDA DAVIDAVIČIENĖ
(2016), Reduction of the Information Asymmetry in Mergers & Acquisitions Through the Means of Payment, Journal of System and Management Sciences, Available in
https://www.aasmr.org/jsms/Vol.6/Vol6_No.2_2.pdf

ERDOS, David
(2019), European Data Protection Regulation, Journalism, and Traditional Publishers, The Development of European Data Protection Law and Regulation, Available in
https://doi.org/10.1093/oso/9780198841982.003.0003

ESAYAS, Samson
(2018), Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers, SSRN Electronic Journal, Available in https://doi.org/10.2139/ssrn.3232701

ESAYAS, Samson
(2018), Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers, SSRN Electronic Journal, Available in https://doi.org/10.2139/ssrn.3232701

EUROPEAN COMMISSION
(2016), Case M.8124 – Microsoft / LinkedIn, Available in
https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf

EUROPEAN COMMISSION. Directorate General for Competition
(2024), Non-Price Competition: EU Merger Control Framework and Case Practice, Publications Office, Available in https://data.europa.eu/doi/10.2763/67590

EUROPEAN COMMISSION. Directorate General for Competition
(2024), Protecting Competition in a Changing World: Evidence on the Evolution of Competition in the EU during the Past 25 Years, Publications Office, Available in https://data.europa.eu/doi/10.2763/089949

EUROPEAN DATA PROTECTION BOARD
(2025), Position paper on Interplay between data protection and competition law, Available in https://www.edpb.europa.eu/system/files/2025-01/edpb_position-paper_20250116_interplay-between-data-protection-and-competition-law_en.pdf

FARRÉU RAMA DOS SANTOS BARATA, Filipe Manuel
(2024), The W&I Insurance as a Facilitating Tool in the Negotiation Process for the Acquisition of a Controlling Shareholding, Revista Electrónica de Derecho, Available in https://doi.org/10.24840/2182-9845_2024-0003_0004

Federal Court of Justice
(2023), September 15, 2023 - V ZR 77/22, Available in https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=15.09.2023&Aktenzeichen=V%20ZR%2077/22

FEDERAL TRADE COMMISSION
(2024), FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches, Available in https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches

FINANCIAL STABILITY BOARD (FSB)
(2023), Stocktake of International Data Standards Relevant to Cross-Border Payments

FINANCIAL STABILITY BOARD (FSB)
(2024), Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments, Available in https://www.fsb.org/uploads/P121224-1.pdf

FREESE, Jan
(1978), The Swedish Data Act, The Swedish Institute: Current Sweden, Available in https://www.ojp.gov/pdffiles1/Digitization/49670NCJRS.pdf

GDPR
(2016), General Data Protection Regulation (GDPR) – Legal Text.

GESLEY, Jenny
(2019), European Union: Collection of Personal Data of Hotel Guests, The Law Library of Congress, Global Legal Research Directorate

HANSSON, Emil
(2024), Data Protection Considerations in Pre-Merger Process: Due Diligence and Merger Assessment, Lund University, Available in https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9180069&fileOId=9182675

ILAN, Daniel / GORRLIEB, Cleary / HAMILTON LLP
(2016), Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities, Harvard Law School Forum on Corporate Governance, Available in https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/

INFORMATION COMMISSIONER OFFICE (ICO)
(2018), Guide to the General Data Protection Regulation (GDPR).

INTERNATIONAL NETWORK OF PRIVACY LAW PROFESSIONALS
(2018), A Brief History of Data Protection: How Did it All Start?, Available in https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

ISSAOUI, Awatef, Jenny Örtensjö, and M. Sirajul Islam
(2023), Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, Future Business Journal, Available in https://doi.org/10.1186/s43093-023-00285-2

KEIL, Sacha
(2021), A Comparative Study on the Role of Non-Price Competitiveness for European Countries, Available in https://www.imk-boeckler.de/data/downloads/IMK/FMM%20Konferenz%202023/v_2023_10_20_keil.pdf

KIM, S. David
(2020), The Valuation Effects of Hotel Mergers, Tourism Economics, Available in https://ssrn.com/abstract=3792332

KLEIDERMAN, Alex
(2024), Spain hotel check-in delay fears as new data rules begin, BBC News, Available in https://www.bbc.com/news/articles/ce9g93p405zo

KPMG LAW
(2023), BGH extends duty of disclosure of real estate sellers, Available in https://kpmg-law.de/en/bgh-extends-duty-of-disclosure-of-real-estate-sellers/

KUMMER, Christopher
(2007), Do Virtual Data Rooms Add Value to the Mergers and Acquisitions Process?, Institute of Mergers, Acquisitions and Alliances

KUNER, Christopher, Lee A Bygrave, Christopher Docksey, and Laura Drechsler
(2020), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Available in https://doi.org/10.1093/oso/9780198826491.001.0001

LAWANTS
(2025), Mergers and Acquisitions (M&A) in Spain: Laws and Regulations, Available in https://www.lawants.com/en/mergers-acquisitions-spain/

LAWANTS
(2025), Spanish Companies Act (Ley de Sociedades de Capital), Available in https://www.lawants.com/en/spain-companies-act/

LEENES, Ronald, Rosamunde Van Brakel, Serge Gutwirth, and Paul De Hert
(2017), Data Protection and Privacy: (In)Visibilities and Infrastructures, Law, Governance and Technology Series, Springer International Publishing, Available in https://doi.org/10.1007/978-3-319-50796-5

LIYANAARACHCHI, G. P., Viglia, G., & Kurtaliqi, F.
(2023), Privacy in hospitality: managing biometric and biographic data with immersive technology, International Journal of Contemporary Hospitality Management, Available in https://doi.org/10.1108/IJCHM-06-2023-0861

LYNN, Kennedy
(2023), The Influence of Loyalty Programs on Hotels, Hospitality Graduate Student Scholarship, Available in https://scholarsarchive.jwu.edu/hosp_graduate/33

MENENDEZ-ROCHE, Marc
(2024), Spain's New Tourist Rules Cause Uproar, EuroWeekly, Available in https://euroweeklynews.com/2024/09/26/spains-new-tourist-rules-cause-uproar/

MINTZ, Levin, Cohn, Ferris, Glovsky and Popeo
(2022), On Sharing and Managing Competitively Sensitive Information in M&A Transactions, Available in https://www.mintz.com/insights-center/viewpoints/2871/2022-09-19-sharing-and-managing-competitively-sensitive-information

MORGAN LEWIS
(2020), Practice Guide: M&A Transactions, Available in https://www.lawworks.org.uk/sites/default/files/files/LW-NFPP-C19-CORP-Merger-detailed-guide.pdf

MORGAN LEWIS
(2023), German Federal Court: Seller Has Increased Duty of Care in Case of a Virtual Provision of Information During Due Diligence Process, Available in https://www.morganlewis.com/pubs/2023/12/german-federal-court-seller-has-increased-duty-of-care-in-case-of-a-virtual-provision-of-information-during-due-diligence-process

NANDA, Akkshay
(2024), Checking In: Privacy and the hotel industry, Available in https://hospitality.economictimes.indiatimes.com/news/speaking-heads/checking-in-privacy-and-the-hotel-industry/116731315

OECD
(2025), Concurrence dans la chaîne d'approvisionnement alimentaire, OECD Competition Law and Policy Working Papers, Available in https://doi.org/10.1787/eeeab061-fr

OECD
(2011), Information Exchanges between Competitors under Competition Law: Key Findings, Summary and Notes, OECD Competition Law and Policy Working Papers, Available in https://doi.org/10.1787/327f7dd3-en

OLDANI, Isabella
(2020), Exchanging and Protecting Personal Data across Borders: GDPR Restrictions on International Data Transfer, University of Trento, Available in https://iris.unitn.it/retrieve/e3835196-da7b-72ef-e053-3705fe0ad821/PhD%20dissertation_Isabella%20Oldani.pdf

PANKAJ, Hrsikesa
(2025), Cybersecurity and Data Privacy in Hospitality and Tourism Industry: Unveiling the Challenges and Risk Mitigation Strategy: A Research Review, International Journal of Science and Research (IJSR), Available in https://doi.org/10.21275/SR25205142950

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
(2024), Chinese Court Releases Landmark Decision on Requirements for Cross-Border Transfer of Personal Information Under the PIPL, Available in https://www.paulweiss.com/media/3985374/chinese_court_releases_landmark_decision_on_requirements_for_cross_border_transfer_of_personal_information_under_the_pipl.pdf

PÉREZ-ORDÓNEZ, Diego
(n.d.), The Guide to Mergers and Acquisitions, Latin Lawyers Insight, Available in https://www.bu.com.co/sites/default/files/2021-02/latinlawyerguidetoma.pdf

PILLAI, Souji Gopalakrishna, Kavitha Haldorai, Won Seok Seo, and Woo Gon Kim
(2021), COVID-19 and Hospitality 5.0: Redefining Hospitality Operations, International Journal of Hospitality Management, Available in https://doi.org/10.1016/j.ijhm.2021.102869

PINHO, Alexandre
(2024), Mergers and Acquisitions on the Hospitality Industry: Strategies and Implications on Post-acquisition, Universidade de Porto.

PORTUGAL
(2019), Lei n.º 58/2019, de 8 de agosto

RAMIC, Meris
(2022), Privacy policies and the GDPR, University of Austria, Available in https://penni.wu.ac.at/supervision/Meris%20Ramic%20Thesis%202022.pdf

ROTH, Alexander / VOIGHT, Paul
(2020), Data Privacy in M&A Transactions, Available in https://www.taylorwessing.com/de/insights-and-events/insights/2020/02/data-privacy-in-ma-transactions

SALAMANCA, Antonio
(2023), Blockchain in the hospitality industry: Identifying main applications, University de les Illes Balears, Available in https://dspace.uib.es/xmlui/bitstream/handle/11201/163003/Salamanca_Fern%C3%A1ndez_Antonio.pdf?sequence=1&isAllowed=y

SÁNCHEZ, Sergio; NOGUER, Alvaro
(2022), Negotiated M&A Guide 2022 Corporate and M&A Law Committee, Available in https://www.ibanet.org/document?id=Corporate-m-a-minority-Spain-22

STAM, Alexandra, and Brian Kleiner
(2020), Data Anonymisation: Legal, Ethical, and Strategic Considerations, FORS Guide, Available in https://doi.org/10.24449/FG-2020-00011

STEFANO RODOTÁ
(2009), Data Protection as a Fundamental Right, Reinventing Data Protection?

TENE, Omer / FITZ SIMONS, Mary / DE SANTIS, Federica / KEENEY, Rachel
(2024), Navigating Privacy and Data Security Challenges in the Hospitality Industry: Key Considerations for Hotel Management Agreements, Available in https://www.goodwinlaw.com/en/insights/publications/2024/09/insights-realestate-navigating-privacy-and-data-security-challenges

TENE, Omer / FITZ SIMONS, Mary / DE SANTIS, Federica / KEENEY, Rachel
(2024), Navigating Privacy and Data Security Challenges in the Hospitality Industry: Key Considerations for Hotel Management Agreements, Available in https://www.goodwinlaw.com/en/insights/publications/2024/09/insights-realestate-navigating-privacy-and-data-security-challenges

TOTH, Gergely
(2022), Preserving control over user data in the hospitality industry with Solid, Charles University, Available in https://dspace.cuni.cz/bitstream/handle/20.500.11956/176270/120427007.pdf?sequence=1&isAllowed=y

TZANOU, M.
(2013), Data Protection as a Fundamental Right next to Privacy? ‘Reconstructing’ a Not so New Right, International Data Privacy Law, Available in https://doi.org/10.1093/idpl/ipt004

VOIGT, Paul, and Axel Von Dem Bussche
(2017), The EU General Data Protection Regulation (GDPR), Springer International Publishing, Available in https://doi.org/10.1007/978-3-319-57959-7

WARREN, Samuel / BRANDEIS, Louis
(1890), The Right to be Let Alone.

YANG, Yun
(2025), Effects of the Size of Acquisition on a Hotel Group’s Financial Performance, Available in https://doi.org/10.7275/KPVX-Q091

YU, Jongsik, Hyoungeun Moon, Bee-Lia Chua, and Heesup Han
(2022), Hotel Data Privacy: Strategies to Reduce Customers’ Emotional Violations, Privacy Concerns, and Switching Intention, Journal of Travel & Tourism Marketing, Available in https://doi.org/10.1080/10548408.2022.2061673

(2022), Yue 0192 Min Chu No. 6486

YURTSEVER, Ali
(2024), Recent Constitutional Court Decision Echoes the Importance of Data Protection in M&A Transactions. Available in https://www.mondaq.com/account/register