DRAFT

Privileged and Confidential

Non-compliance of Booking.com with Digital Markets Act obligations

- Article 5(7) DMA prohibits Booking.com from requiring end users to use, or business users to use, to offer, or to interoperate with its payment system in the context of services provided by business users using Booking.com's CPS.
- Article 6(10) DMA grants businesses users access rights to data related to their use of Booking.com's core platform services and to request from Booking.com free of charge, permanent real-time access to data provided for or generated by them and their customers in the context of the use of the relevant core platform services.
- According to Articles 13(3) DMA compliance with Articles 5(7) and 6(10) DMA lies with the gatekeeper.
- Articles 13(4) (anti-circumvention provisions) plays an important role to counter deceptive user interfaces and ensure effective compliance with the prohibitions in Articles 5(7) and 6(10) DMA.

I. Article 6 (10) – Access to data

Hotels must make the best use of data available to communicate with guests to offer more services available during their stay for example, but also to attract new customers and improve their profitability. Without data they cannot communicate, analyse and improve their overall performance. Such crucial information in online distribution cannot stay exclusively in the hands of the gatekeeper. At the end of the day, hotels are the one hosting and servicing the guests. The contact information of the guests (e.g., email addresses) and in particular their financial data is and will be key for the hospitality sector's growth,

digitalisation and economic performance. Finally, hotels also have no say in their data being shared through Booking's affiliate network from which hotels cannot opt out.

A. What data Booking.com provides by default

Booking.com provides hotels with access to both non-aggregated and aggregated data to support operational and strategic decision-making. **Non-aggregated** data includes guest names, nationality, reviews, and messages. Credit card information is accessible only within a protected area governed by security policies, and only if the hotel does not participate in the Payments by Booking.com service. Additional guest-provided details may include arrival time, bed preferences, age group, allergies, interests, and special dietary requirements. **Aggregated data** is available through analytics tools and includes statistics based on reservations, market comparisons with a self-defined competitive set of at least ten hotels, and year-over-year performance metrics. This data covers indicators such as length of stay, device usage, top guest origin countries, traveler type (e.g., international, domestic, business, leisure), cancellation rates and policies, room nights, room revenue, average daily rate, search result views, property page views, conversion rate, review score, and property page score. Some data is presented in graphical format without numerical values, specifically when sourced from Booking.com as a channel.

B. What data hotels do not have access to

Despite the data currently provided by Booking.com, hotels require access to additional datasets, outlined below, in accordance with the objectives of DMA, to promote fairness and contestability in digital markets:

a. Guest Data – E-mail, telephone/mobile number

Hotels must be granted access to guests' complete contact details, including unmasked email addresses and telephone or mobile numbers. This information is actively provided by the end user during the booking process and is indispensable for hotels to directly (i) communicate with guests, (ii) confirm reservations, (iii) manage check-ins, (iv) provide post-stay services, (v) optimize guests' stay (offering a tailormade stay, offering targeted services according to the guests necessities), and most importantly (vi) communicate 3-D secure payment-links to process the payment outside of Booking's ecosystem. Denying hotels access to these unmasked details would undermine compliance with Article 6(10), which clearly establishes that personal data directly connected to the user's transaction must be shared with the business user once valid consent is obtained. Without this information, hotels are forced to use Booking.com's internal communication system, making them more dependent on its ecosystem.

b. Guest Data – Channel data

Hotels need access to information on the source of each reservation, including whether it was made directly on Booking.com or through one of its affiliates. This should include the name of the affiliate, its type (e.g. travel agency, online travel agencies, global distribution systems), and any other available data

identifying the source of the booking. This data enables hotels to understand the structure of the OTA ecosystem, assess the value of different distribution channels, and improve their commercial strategy. Aggregated channel data would also help hotels better understand the balance between their B2C and B2B business, information they would naturally have access to if the reservation had not gone through an intermediary. The draft guidelines on the interplay between the DMA and the GDPR by the European Data Protection Board (EDPB) and the Commission also explicitly identifies "business performance data" and "end user engagement data" as falling within Article 6(10)'s scope, to be made available "at a level of granularity that provides the most utility to business users." Channel data, indicating whether a reservation originated directly through Booking.com or through an affiliate partner, fits squarely within this definition. It is data generated through the activity of the business user and the end user in the context of the CPS and directly connected to the booking transaction.

c. Guest Data – IP Address and geo-location

Hotels need the IP address or geo-location data associated with each reservation. If a booking had been made directly through a hotel's own website, such data would automatically be available to the hotel. The draft joint DMA–GDPR guidelines explicitly confirm that Article 6(10) DMA covers "other data that is processed (including automatically) by a core platform service, such as IP address and location data." This language leaves no doubt that the IP addresses and geo-location data collected by Booking.com in connection with a transaction fall squarely within the scope of the DMA's data access obligation.

d. Financial Data – Payment information

For hotels that use the "Payments by Booking.com" system, it is essential to access aggregated data on the methods of payment used by guests, including the proportions of payments made by credit card, bank transfer, or national mobile payment systems. This data allows hotels to evaluate the actual value and performance of Booking.com's payment services. The draft joint guidelines identify payment services as a key example of "services provided together with, or in support of, a core platform service," and explicitly mention "end user payment history" among the data that must be made available to business users.

C. Limitations in Booking.com's compliance with Article 6(10) DMA on data access for hotels

The DMA and the draft joint guidelines issued by the European Commission and the European Data Protection Board (EDPB) clearly establish that business users, such as hotels, must be able to specify the data, including personal data, they wish to access under Article 6(10) DMA. Gatekeepers are required to provide business users and their authorised third parties with transparency and control over such data, allowing them to determine the specific datasets, their level of granularity, and the purposes for which they are requested. Access must cover both aggregated and non-aggregated data, including personal data, provided that the end user has given valid consent under the GDPR. However, Booking.com's current

practices do not fully meet these legal obligations. The platform limits the extent hotels can exercise their rights under Article 6(10) DMA for three main reasons:

1. It does not allow hotels to access additional data beyond what is provided by default and lacks functionalities to make specific requests under the DMA.
2. It prevents hotels from customising consent requests to end users in order to obtain personal data.
3. It misuses the concept of the "acquired user" to justify withholding key guest data, such as unmasked email addresses.

1. Lack of access to data beyond what Booking.com provides by default

Booking.com does not offer hotels any additional functionalities or interfaces to customise and specify the data accessible through the standard channels available, namely, the Extranet and an optional API connection via a channel manager or property management system (PMS) beyond the limited data provided by default. (see Section I).

All relevant data, including personal data, is currently accessible to hotels only through:

- the Extranet panel ("Reservations" section),
- guest messages sent through the Booking.com system, or
- data automatically transferred via the channel manager.

No dedicated interface exists for hotels to make specific data access requests as foreseen by Article 6(10) DMA. If hotels need additional information, they can only contact Booking.com directly, without any guarantee of obtaining the requested data. These cases are handled individually, and Booking.com frequently invokes its own privacy policy to deny access, rather than addressing its obligations under the DMA. As a result, hotels are effectively denied the ability to request and access the full range of data they are legally entitled to, limiting their capacity to manage customer relationships, improve their services, and comply with data protection obligations.

2. Inability to customise consent requests for personal data

Booking.com does not allow hotels to customise, review, or influence the consent mechanism through which guests authorise the sharing of their personal data under Article 6(10) DMA. Booking.com solely determines the essential elements of the consent flow, including:

- which data categories are requested (e.g. name, phone number, partially anonymised email address);
- how, in what terms, and at what moment guests are informed and asked to consent.

This goes far beyond interface design. By controlling all substantive aspects of the consent request, Booking.com does not provide hotels with the possibility to determine the data and purposes for which

consent is sought, even though Recital 60 DMA and the DMA-GDPR draft guidelines require that business users must be placed in a position to obtain consent themselves and decide these elements.

At the same time, the DMA-GDPR draft guidelines assign responsibility for obtaining valid consent to business users, i.e. hotels. This creates a structural inconsistency with Booking controlling both means and purposes of collecting consent, while hotels bear the entire legal responsibility for its validity.

3. Misuse of the "acquired user" concept to withhold data

Booking.com also relies on a flawed interpretation of the **"**acquired user" concept in Recital 40 DMA to justify withholding essential guest data, particularly unmasked email addresses. The platform claims that providing such data would allow hotels to contact guests directly and thereby "bypass" Booking.com, leading to lost commissions.

However, Recital 40 clearly establishes two cumulative conditions for an acquired end user:

1. The end user has entered into a commercial relationship with the business user; and
2. The gatekeeper has been remunerated (directly or indirectly) for facilitating that acquisition.

In relation to the first condition, the notion of a commercial relationship is not defined, but point 2.4.2 of the Booking.com's General Delivery Provisions (GDP) mentions *"by making a reservation through the Platform, a direct legal contract is created between the accommodation and the Guest"*. Accordingly, a contract has been concluded even if an end user benefits from the option of free cancellation. In relation to the second condition, the question is when the commission to the gatekeeper is legally due, independently of the conditions and date of the actual financial transfer. Booking.com considers a user acquired and remuneration due when a reservation is made. According to point 2.2.1 of the Booking.com GDP, the accommodation shall pay a commission when a reservation is made, even in case of overbooking or cancellation. If this is the time a user is considered acquired, this then means that Booking.com ought to provide the guest's email to hotels at this time as hotels will have paid the commission already, so there is no free-riding issue anymore. However, it transpires that guests have two payment options. Depending on which option the guest chooses, it has an impact on when a user can be considered acquired.

On Booking.com, the guest has the choice between two payment options:

- Option one is a non-refundable reservation. In such a case, the accommodation and Booking.com are remunerated when the reservation is made. This means that the two conditions of recital 40 DMA are met and the end user is acquired upon reservation and payment. At this point in time, Booking.com should stop withholding the guest's email as there is no longer a freeriding issue.

- Option two is a reservation with free or conditioned cancellation and payment at the hotel[1]. In such a case, the accommodation is paid when the check-in is done, but the commission to Booking.com is due when the period cancellation has expired. This implies that the user is acquired at the end of the cancellation period and not at the moment of the check-in. Different hotels have different cancellation policies, there is no universal rule on cancellation in Booking.com's GDP.

In both cases, once the commission is due, Booking.com's justification for withholding guest data no longer applies. Yet, in practice, Booking.com continues to withhold such data indefinitely without explanation or merely citing privacy concerns that have no legal basis once consent has been obtained and the acquisition criteria are met. This selective interpretation of "acquired user" undermines the spirit and objectives of the DMA, which aim to prevent gatekeepers from using their market position to restrict fair access to essential business data.

Beyond these legal considerations, it is also important to recognise the moment at which the guest's choice is effectively made. When a customer confirms a reservation, they are no longer browsing for accommodation in a given location, they are selecting that specific hotel for their stay. From that point onwards, the guest–hotel relationship is established in substance as well as in law, further reinforcing that the hotel should not be prevented from accessing essential guest data once the acquisition conditions under Recital 40 DMA are fulfilled.

I. Article 5 (7) - Payment systems

Booking.com charges hotels a commission fee for every reservation made through its platform. These fees range from 13% to 30%, sometimes up to 40%, depending on various factors like the country of registration, property location, type, cancellation policy, and payout method. For hotels, the base fee is 15%, which can rise to 18% if using Booking.com's recommended member service.

A. Restrictions on alternative payment systems

A.1 Summary of consequences of Booking.com's restrictions for hotels

1. **High commission fees**: Hotels pay between 13% and 30% (sometimes up to 40%) per booking, reducing profit margins significantly.
2. **Additional commission increases**: Extra fees of 1.1% to 3.1% can be applied on top of the base commission, further eroding profitability.

[1] In this specific case, the customer is no more committed to Booking than to the hotel, since neither of them is being paid. Therefore, Booking has no grounds to obstruct.

3. **Restricted payment options**: Hotels cannot use alternative payment systems or send 3-D Secure links via Booking.com's messaging system.
4. **Forced reliance on Booking.com payments**: Limitations on direct payment methods create dependency on Booking.com's payment program.
5. **Compliance risks with PSD2/SCA**: Card-not-present transactions are increasingly prohibited, leaving hotels vulnerable to chargebacks and refunds.
6. **Loss of control over prepayment policies**: Planned discontinuation of direct prepayment options forces hotels to adopt Booking.com's system.
7. **Operational inefficiencies**: Payment links often blocked or distrusted by guests, leading to unguaranteed reservations and increased fraud risk.
8. **Limited customization**: Hotels cannot set their own booking, cancellation, or payment conditions in the extranet, reducing flexibility and competitiveness.
9. **Reduced innovation and competition**: External payment providers are sidelined, limiting hotels' ability to choose cost-effective or secure solutions.

A.2 Constraints on non-Booking.com payment methods

Booking has adopted a strategy which restricts business users from using alternative payment systems, which violate Art. 5(7) DMA.

Indeed, because 3-D secure payment links cannot be sent via Booking.com's internal communications system to guarantee reservations, hotels can only charge guests in advance through bank transfers or card-not-present (CNP) transactions. Many hotels may in practice be prevented from processing unsecured payments, if their acquiring bank or card processor prohibits or restricts high-risk CNP transactions. As a result, the hotel is effectively trapped, with no viable way to charge the guest directly, and is therefore almost forced to rely on Booking.com's own payment solutions. This restriction not only creates a dependency on Booking.com's payment program and by extension the automatic price adjustments-mechanism that circumvent the ban on price-parity requirements, but it undermines competition and innovation by external payment providers.

Moreover, Booking.com has already announced on its website[2] that it plans **to stop supporting prepayment policies that allow hotel partners to charge guests directly** in several countries. This would compel users in these markets to use Booking.com's platform and payment system, violating Article 5(7) of the DMA.

[2]https://partner.booking.com/en-gb/help/policies-payments/payment-products/enhancing-prepayment-policy-security-greece-ireland-and-poland

When a booking is made via Booking.com for a pre-paid stay outside of the Payments by Booking.com's eco-system, the guest provides their credit card details to Booking.com who forwards them to the hotel. The card can then be charged in CNP/MOTO mode (Mail Order / Telephone Order) by manually entering the card number into the terminal. Under the Payment Service Directive 2 (PSD2) and the mandatory Strong Customer Authentication (SCA) card-not-present transactions are more and more not permitted by acquirers and banks. If the client disputes the transaction, they are automatically refunded without the hotel being able to provide proof of good faith.

If the hotels want to process the payments themselves and do not want Booking.com to handle the payment, many hotels use the option of a payment link, which they send to guests—after receiving the booking data from the OTA — to confirm the payment. However, this is an additional action and, from the guest's perspective, not connected to the original booking, which means not all guests will trust the link or complete authentication. It implicates additional security risks and it is vulnerable for fraud (phishing). OTA bookings present an added complication: **Booking.com does not pass on the guest's email address to hotels, and the communication between hotel and guest is only possible via Booking.com's internal messaging systems. This system often blocks external links, so there is a high likelihood that the guest will not receive the payment link at all.** Furthermore, the hotel has no option to insert its own booking/cancellation/payment conditions through the extranet. There is a limited number of items to choose from to set its conditions, but these options are restrictive. For example, a hotelier who wants to record a reservation with a prepayment cannot specify on the extranet that the guest will be sent a 3DSecure payment link or their IBAN for payment purposes. As a result, the customer often lacks trust when receiving payment requests from the hotelier, does not validate the prepayment, and the reservation is therefore not guaranteed.

B. Compliance solutions

- Business users (hotels) should always have the free choice, if the payment is facilitated by Booking.com, to select a virtual credit card (by the Booking Holdings Financial Services) or if they want to facilitate the payment via the hotels own payment services/system. Booking.com should make the costs and implications of selecting such a service clear to its business users. Additionally, hotels should be able to define their reservation and guarantee conditions during the booking process, so that guests are fully informed at the time of confirming their reservation. Importantly, the choice of the payment cannot affect the ranking of the hotel.
- Ideally, the online booking portals would request authentication from the guest directly at the time of booking for bookings where payment is processed via the hotel, create an authorisation token and forward this token together with the card number and the booking to the hotel's systems. The

hotels could then charge the credit card as a Merchant Initiated Transaction (MIT) without any problems and without the risk of a chargeback.

- End users and business users must not be disadvantaged if they wish to use the hotel's own /direct payment methods. The choice of the payment services cannot affect the ranking of the hotel.
- Booking.com should clearly display different payment options available to end users (i.e. credit card, debit card, PayPal, Apple pay, banks, etc). End users must be free to choose which payment system they would like to use to make their accommodation reservation.
- Booking.com should be banned from mandating the usage of Virtual Credit Cards or forcing or bundling their usage with other services, thereby tying their intermediation service to their payment system. Booking.com should not dictate the method by which the guest should pay the hotel. Currently, Booking.com does not allow sending payment links or QR codes with payment links to clients through its platform, except under exceptionally strict conditions, so they could pay their reservation directly to the hotel in an environment where payments are secure and prevent fraud. (Simply downloading the payment in the terminal without the presence of the card will be refunded by the bank in case of a client's claim, which causes a problem for non-refundable reservations).
- Booking.com should explicitly state and guarantee that opting in or out of payments by booking or pre-payments won't affect ranking, neither directly nor indirectly.

c. Conclusion

Booking.com has built an ecosystem that ultimately restricts the possibility for hotels to communicate with their guests and promote offers to end-users outside the Booking.com's platform including sending links to alternative payment systems. This is not compliant with Art. 6(10) DMA and Art. 5(7) DMA.