About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hospitality professionals and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hospitality venues, and create a healthy ecosystem of technology suppliers.

Copyright 2018, Hospitality Technology Next Generation

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

For any software code contained within this specification, permission is hereby granted, free-of-charge, to any person obtaining a copy of this specification (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the above copyright notice and this permission notice being included in all copies or substantial portions of the Software.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hospitality Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hospitality Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hospitality Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.
Table of Contents

1 DOCUMENT INFORMATION .............................................................................................................. 5
  1.1 CONTRIBUTORS .......................................................................................................................... 5
  1.2 USEFUL RESOURCES ................................................................................................................. 5
  1.3 AUDIENCE ................................................................................................................................... 5
  1.4 OVERVIEW .................................................................................................................................. 6

2 IS THE GDPR APPLICABLE TO YOU? .......................................................................................... 7
  2.1 PROVISIONS OF THE GDPR ...................................................................................................... 7
  2.2 ROLES AND RESPONSIBILITIES UNDER THE GDPR ............................................................... 7
    2.2.1 The data subject ...................................................................................................................... 8
    2.2.2 Rights of the data subject ....................................................................................................... 8
    2.2.3 The supervisory authority ....................................................................................................... 8
    2.2.4 The data protection officer ..................................................................................................... 8
    2.2.5 The data controller .................................................................................................................. 8
    2.2.6 The data processor .................................................................................................................. 9
  2.3 APPLICABILITY OF THE GDPR TO A HOSPITALITY COMPANY ........................................... 9

3 WHAT THE GDPR MEANS TO ROLES AND FUNCTIONS IN THE INDUSTRY ............................ 11
  3.1 CHIEF INFORMATION OFFICERS ................................................................................................. 11
  3.2 CHIEF INFORMATION SECURITY OFFICERS ............................................................................... 12
  3.3 MARKETING MANAGEMENT ...................................................................................................... 12
  3.4 HUMAN RESOURCES MANAGEMENT ....................................................................................... 13
  3.5 SYSTEM VENDORS ..................................................................................................................... 13
  3.6 LEGAL DEPARTMENTS ................................................................................................................ 14
  3.7 GENERAL MANAGERS AND ON-PROPERTY MANAGEMENT ..................................................... 14
  3.8 FRANCHISORS AND FRANCHISEES ......................................................................................... 15
  3.9 DATA PROTECTION OFFICER REQUIREMENTS ......................................................................... 16
    3.9.1 When are DPOs necessary? ...................................................................................................... 16
    3.9.2 Role of the DPO ....................................................................................................................... 16
    3.9.3 Tasks of the DPO (Art. 39) ....................................................................................................... 16
    3.9.4 Expertise and professional qualities ......................................................................................... 16
  3.10 HOW CAN YOU TELL HOW READY YOU ARE? ...................................................................... 17
  3.11 CONCLUSION .............................................................................................................................. 17

4 CUSTOMER RIGHTS FROM A GUEST CENTRIC POINT OF VIEW .................................................. 18
  4.1 DEFINITIONS ............................................................................................................................... 18
  4.2 GDPR – CUSTOMER RIGHTS ..................................................................................................... 18
    4.2.1 The right to be informed ......................................................................................................... 18
    4.2.2 The right of access .................................................................................................................. 19
    4.2.3 The right to rectification ......................................................................................................... 19
    4.2.4 The right to erasure ............................................................................................................... 19
    4.2.5 The right to restrict processing ............................................................................................... 19
    4.2.6 The right to data portability ................................................................................................... 19
    4.2.7 The right to object .................................................................................................................. 19
    4.2.8 Rights relating to automated decision making and profiling ................................................ 19
    4.2.9 Breach notification ............................................................................................................... 19
    4.2.10 Accountability and governance ............................................................................................. 20
    4.2.11 Legacy data ........................................................................................................................... 20

5 RISKS OF DATA LOSS & OBLIGATIONS ....................................................................................... 21
  5.1 POWER OF SUPERVISING AUTHORITIES TO IMPOSE CORRECTIVE MEASURES ..................... 21
  5.2 IMPOSITION OF ADMINISTRATIVE FINES BY THE SUPERVISING AUTHORITY ........................ 21
5.3 Jurisdiction for corrective measures when the data controller or processor operates in more than one Member State ................................................. 22
5.4 Jurisdiction for corrective measures when the data controller or processor is not located in the EU ......................................................... 23
5.5 Schedule A ........................................................................................................ 23
5.6 Schedule B ........................................................................................................ 23
5.7 Undue delay ........................................................................................................ 25

6 Data transfer across borders and data governance ................................................. 27

6.1 Conditions that allow data transfer outside the EEA ......................................... 27
6.2 Model clauses ..................................................................................................... 27
6.3 Consent ............................................................................................................... 27
6.4 Public interest ..................................................................................................... 27
6.5 Binding corporate rules ....................................................................................... 28

7 Relationship between PII Code of Conduct and GDPR ........................................ 29

8 Guest data flow and GDPR implications ............................................................... 30

8.1 Assumptions ...................................................................................................... 31
8.2 Commentary to the flow-chart ......................................................................... 31
8.3 GDPR role(s) .................................................................................................... 32
  8.3.1 Controller-A (Hotel) ...................................................................................... 32
  8.3.2 Controller-B (Brand) .................................................................................... 32
  8.3.3 Processor (CRS) .......................................................................................... 33
  8.3.4 Controller-C (Distributor) ............................................................................. 33
  8.3.5 Data flow ....................................................................................................... 33
  8.3.6 Agreements required .................................................................................... 34
  8.3.7 Consent ......................................................................................................... 35

8.4 Use cases/Scenarios ......................................................................................... 36
  8.4.1 Direct booking at the hotel (or even a walk-in) ............................................ 36
  8.4.2 Call Centre Direct (mainly voice call or e-mail) ......................................... 37
  8.4.3 Online direct via own website connected to the branded or unbranded CRS ......................................................... 37
  8.4.4 OTA or other intermediary (including physical travel agency booking via GDS or the web) ................................. 37
1 Document Information

1.1 Contributors
While over 50 companies participated in the HTNG GDPR for Hospitality Workgroup, this document was primarily written by the following persons & companies:

<table>
<thead>
<tr>
<th>Author</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Bell, co-Chair</td>
<td>AjonTech, LLC</td>
</tr>
<tr>
<td>Chris Farrar, co-Chair</td>
<td>Exceptional Innovation</td>
</tr>
<tr>
<td>Daniel Johnson, co-Chair</td>
<td>VENZA</td>
</tr>
<tr>
<td>Richard Sheinis, co-Chair</td>
<td>Hall Booth Smith, P.C</td>
</tr>
<tr>
<td>Chris Airey</td>
<td>Airangel Limited</td>
</tr>
<tr>
<td>Bill Beckler</td>
<td>Alice</td>
</tr>
<tr>
<td>Stephen Clay</td>
<td>Agilysys</td>
</tr>
<tr>
<td>Patrick Foley</td>
<td>Marriott International</td>
</tr>
<tr>
<td>Charles Helleputte, Diletta De Cicco</td>
<td>Mayer Brown</td>
</tr>
<tr>
<td>Robbie Laack</td>
<td>Kalahari Resorts</td>
</tr>
<tr>
<td>Thomas Linder</td>
<td>Infor</td>
</tr>
<tr>
<td>Jeffrey Parker</td>
<td>Red Lion Hotels</td>
</tr>
<tr>
<td>Kris Troukens</td>
<td>Safe Hotels</td>
</tr>
<tr>
<td>Finn Schulz</td>
<td>Independent Consultant</td>
</tr>
<tr>
<td>Bryan Steele</td>
<td>Jireh-Tek, Ltd.</td>
</tr>
<tr>
<td>Suzanne Ward</td>
<td>Movenpick Hotels</td>
</tr>
</tbody>
</table>

1.2 Useful resources
All HTNG best practices, software specifications, whitepapers and other general resources can be found at this link: [http://www.htng.org/?page=technical_specs](http://www.htng.org/?page=technical_specs).

1.3 Audience
This Introduction is intended to address the needs of a broad audience within the industry and its ecosystem, both at corporate and property levels. Some roles and functions expected to benefit from this document:

- Chief Information Officers
- Chief Information Security Officers
- Marketing management
- Human resources management
- IT managers
System vendors
Legal departments
General managers and other on-property management
Franchise managers

There are other roles outside of this list who will need to abide by the GDPR. If an employee touches, manages or makes decisions about personally identifiable information, they need to be aware of the GDPR and should use this document for reference.

1.4 Overview

In April 2016, the European Union adopted the General Data Protection Regulation (GDPR). The purpose of the GDPR is to lay the ground rules for a thriving informative economy within the EU while more thoroughly protecting the personally identifiable information of EU citizens.

The Regulation goes into effect on May 25, 2018. At that time, it will replace the EU’s earlier Data Protection Directive (1995).

The GDPR covers both employees and guests. This white paper will be principally concerned with its impact on the handling of guest data. Where appropriate, though, the document will also discuss employee information. In general, HTNG encourages companies to take a holistic view of the problem of data security; and to develop strategies, policies, processes and protections for all forms of personally identifiable information.

The purpose of the HTNG GDPR for Hospitality Workgroup is to help the audience understand what they need to be thinking about and planning for. This introductory chapter will provide readers with a general orientation. The body of the while paper and the companion materials will offer more in-depth guidance.

The efforts of the workgroup build on those of the previous HTNG Personally Identifiable Information (PII) Workgroup, which developed a set of materials around the management and protection of PII. This included a statement of principles, a code of conduct, a self-assessment instrument and more. We encourage you to consult these for more background on the issues and approaches involved in dealing with the kind of data within the scope of the GDPR.
2 Is the GDPR Applicable to You?

If your company or your property operates, directly markets to, or offers services in the European Union or belongs to a chain, management company or ownership group that does business in the EU, then yes, the GDPR is applicable to your company. Any company that offers goods and/or services to European residents needs to comply with the Regulation whether or not they’re located in the EU. Failure to comply exposes the company to large fines.

HTNG believes it is highly advisable for all companies operating in the industry to acquaint themselves thoroughly with the Regulation’s provisions. The current document will help, as will the companion documents. You can also review the information on the GDPR website¹.

2.1 Provisions of the GDPR

The main provisions of the GDPR cover these areas:

- **Personally Identifiable Information (PII):** The definition of the kind of personal data covered by the regulation has been expanded to now include online identifiers and other elements that can be used to identify a natural person when combined.
- **Extra-territoriality:** It is applicable even when an organization is not located in the EU, but does business, directly markets, etc. in the EU.
- **Monetary penalties:** There are stiff penalties for non-compliance of up to 4% of a company’s annual revenue.
- **Lawful basis for use:** There must be a lawful basis for collecting and using an individual’s personal data. Article 6 of the Regulation defines six such lawful bases with one being **consent** (next).
- **Consent:** When the other lawful bases do not apply, use of peoples’ personal data must be with their explicit consent. They must be able to withdraw consent as easily as they give it.
- **Transparency:** People must be able to determine whether, how and why their personal information is being used. Individuals must be able to get a copy of the data being held on them.
- **Right to modify:** Individuals have the right to demand their data be changed, corrected or deleted.
- **Portability:** People have the right to easily move their data from one service provider (e.g. a hotel chain) to another.
- **Security-by-design:** Systems need to be designed from the start with data and privacy protection as a key design principle.
- **New roles and responsibilities:** The Regulation defines new roles and responsibilities for organizations like hotels and technology vendors, which use or manage individuals’ personal data.
- **Notification:** In the case of data breaches, organizations must notify a supervisory authority within 72 hours.

2.2 Roles and responsibilities under the GDPR

The GDPR defines certain specific roles to help in the management and protection of personal data. These roles have some defined responsibilities and (in the case of natural persons) defined rights.

¹ https://www.eugdpr.org
2.2.1 The data subject

The data subject is the guest or employee, the natural person whose information needs to be protected.

2.2.2 Rights of the data subject

The rights of the data subject under the GDPR are extensive and detailed. These rights are presented more in depth in the section “Customer Rights from a Guest Centric Point of View.” The complete, detailed list can be found in Articles 12 through 23. This is a high-level description:

- The right to understand what data is being collected, what it will be used for and how long it will be held.
- The right to explicitly consent to the use of their data and the right to easily withdraw consent.
- The right to restrict the reason(s) for how the data will be used.
- The right to review, modify, correct and delete the information held about them.
- The right to be forgotten – that is, to have their data deleted.
- The right to obtain a copy of their data in a common machine-readable format, and to transfer it to another Data Controller (see Section 2.2.5 below).

2.2.3 The supervisory authority

The supervisory authority is the governmental officer or agency that the GDPR directs to oversee GDPR compliance in each EU member state.

2.2.4 The data protection officer

The data protection officer (DPO) is an organization’s personal data advocate, involved with all issues relating to the protection of personal data. Further details will be evaluated in the DPO section (see Section 3.9). A data protection officer is mandated for companies whose principal business is monitoring, processing or storing personal information and doing so in large volumes.

2.2.5 The data controller

A data controller determines the purposes for how the data will be used, collects the data and establishes the means by which it will be processed.\(^2\)

Responsibilities of the data controller include:

- Understand the nature of the data being captured and used.
- Understand the severity of the risk to the guest (employee) should the data not be adequately protected.
- Implement appropriate technical and organizational measures commensurate with that risk to ensure that the data is being handled as required under the Regulation.
- Similarly, implement data protection principles to integrate necessary protections and safeguards into the processing of the data as required by the Regulation and to protect the rights of guests.
- Collect and process only the data necessary for the immediate business purpose and make it available only to those who need it.
- Work only with data processors that operate in compliance with the Regulation.
- Review and update these measures as necessary.

\(^2\) Article 4, paragraph 7 of the Regulation
\(^3\) Chapter IV, Section 1, Articles 24 & 25: Responsibility of the Controller; Data protection by design and by default. Also Article 28.
2.2.6 The data processor

The data controller may also work with or contract with a data processor. This data processor uses the guest data to accomplish various business purposes, some of which may not necessarily be related directly to the immediate purpose of the data that was collected from the guest. So, a hotel may collect the guest's name, credit card information, email address and so forth for the purpose of providing the guest with a room. However, the hotel gives that information to a data processor when providing it to an email marketing agency for a promotional campaign.

Responsibilities of the data processor:

- Act only on the data controller's documented instructions.
- Impose confidentiality obligations on all personnel involved in the processing.
- Ensure the security of personal data.
- Impose the same confidentiality and security provisions on subcontractors as they themselves are subject to; and restrict the activities of the subcontractors to those explicitly contracted for by the data controller.
- Comply with the rights of data subjects.
- Return or destroy the personal data – as requested by the data controller – at the end of the contracted work.
- Provide the data controller with any and all documentation necessary to demonstrate compliance with the Regulation.
- Promptly notify the data controller of any data breach.

Note, that it is possible for the Data Controller and the Data Processor to be the same party.

2.3 Applicability of the GDPR to a hospitality company

The purpose of this section is to address the territorial scope of GDPR, and more specifically, its potential application to hospitality venues which are physically located outside the EU.

Chapter 1, Article 3 of the GDPR states:

1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to;

   a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subject in the Union; or

   b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where member state law applies by virtue of public international law.
This section shall focus on the interpretation of Section 2(a) above for the purposes of whether individual hotels, or hotel companies, physically located outside the EU, are subject to the GDPR. The requirement for applicability of the GDPR to hotels located outside the EU can be broken down into two elements. First, the Regulation applies to the processing of personal data of data subjects who are in the Union. The requirement that the data subject be in the EU would seem to exclude the scenario in which a resident of the EU travels to another region, and subsequently makes a room reservation, or pays for a room. In such case, the data subject is not in the EU.

The scenario more likely to occur is one in which a person in the EU makes a reservation for a room in a hotel outside the EU. In such a scenario, the GDPR would apply to the hotel only if the hotel is offering its goods or services to data subjects in the EU. The GDPR offers very little guidance as to what constitutes the "offering of goods or services" in the EU. The only guidance can be found in Paragraph 20 of the Recitals to the GDPR, which states, in part:

- In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more member States in the Union. Whereas the mere accessibility of a controller's or an intermediary website in the Union or of an e-mail address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users who are in the Union, may make it apparent the controller envisages offering goods or services to such data subjects in the Union.

The determination of whether a hotel outside the EU is subject to the GDPR will have to be done on a case-by-case basis, based upon the factors cited above. In addition to these factors, hotels and other hospitality venues should be aware that the use of third-party booking sites, or vendors that provide third-party marketing services can potentially be viewed as offering goods or services to data subjects in the EU. These third-party marketing services may include individuals accessing their website, using other mechanisms to monitor the browsing behavior of website visitors or even placing cookies on the devices of website visitors. Depending on the website monitoring and tracking that is done, it could possibly qualify as "the monitoring of their behavior as far as their behavior takes place within the Union."

- In the scenario in which a reservation is made from the EU for a USA-based hotel, where the hotel website was clearly targeting European business, there is still the question of which activities should be covered by the GDPR. Is it what happens at the hotel, or is it just the information collected during the booking process? This question will be looked at on a case-by-case basis and the GDPR is not entirely clear.
3 What the GDPR Means to Roles and Functions in the Industry

In whichever role you play in the industry, it will be beneficial to ask yourself a number of questions:

1. Do you understand what personally identifiable information is as it’s defined by the GDPR?
2. Do you understand all of the ways personal data, especially guest data, are collected, managed, monitored, processed or used in the functions for which you are responsible?
3. Do you know who is responsible for each of those activities?
4. Do you understand how personal data is being protected, or how it is failing to be protected?
5. Do you understand the Regulation’s concept of data subject consent and where it applies in your processes?
6. Do you have a mechanism through which the guest or employee can easily and explicitly grant consent; and just as easily and explicitly withdraw it?
7. Have you analyzed the gaps that could expose you to penalties under the regulation?
8. Do you have plans for remedying the gaps? Plans may include:
   1. Training programs for new staff along with ongoing refresher training
   2. Process development or modification
   3. Modification of vendor contracts and even (possibly) replacement of systems or service providers that create significant compliance exposures
9. Do you have a documented and approved Code of Conduct?\(^4\)
10. Do you have plans and processes for ongoing monitoring of compliance?
11. Have you assigned your staff formal responsibilities in connection with compliance?
12. Do you understand your responsibilities under the Regulation in the event of a data breach, and do you and your staff have a documented plan for carrying out those responsibilities?\(^5\)
13. Do you have a process for documenting your compliance with the Regulation in the case of an audit conducted by a supervising authority or other authorized party?\(^6\)

HTNG’s GDPR for Hospitality resources will help with all of this, as will the resources identified in the footnotes of this document.

3.1 Chief Information Officers

If you are a CIO, you should ask yourself the following questions:

- Do you know whether your organization is exposed to the requirements of the Regulation?
- Have you done a risk assessment based on your geographic location and the extent to which you market your services in the EU?
- Do you know which of this information traverses national borders and how?
- Do you have data governance policies and controls in place?
- Do you have a comprehensive listing, data mapping and flow analysis for all PII used by your organization, whether for guests, employees or business partners?
  - Do you know where it initially came from in terms of country of origin, business processes, partner/supplier relationships and more?
  - Do you know all of the systems and databases where the data is stored?

\(^4\) Article 40
\(^5\) Articles 33 & 34
\(^6\) See especially Article 30 paragraphs 1, 3, 4, 5
Does the flow analysis cover movement across national or EU boundaries?

Do you know which data collection, management and processing activities are conducted in-house, and which are outsourced?

- Do you know the contractual provisions under which outside processing takes place and whether they're compliant?
- Do you have processes in place for obtaining and documenting consent? Are they compliant with the requirements of the Regulation?
- Do you have mechanisms which will allow data subjects to easily withdraw consent? Can you then follow through appropriately, deleting the data in response?
- Do you have mechanisms which will allow data subjects (guests or employees) to review the data you're holding on them and correct, modify or delete it? Can you pass such requests on to third-parties who you have engaged to help carry out these responsibilities?
- Do you have auditable logs to be able to demonstrate you have complied with these requirements?
- Do you know how the systems that store PII are safeguarded, how current the protections are and how thoroughly the security processes are being executed? Do you know who is responsible for their security and how qualified they are?
- Do you have mechanisms which will allow data subjects to easily withdraw consent? Can you then follow through appropriately, deleting the data in response?
- Do you have mechanisms for identifying and deleting aged or unneeded data?

### 3.2 Chief Information Security Officers

As a Chief Information Security Officer, you should be able to answer the questions pertaining to Chief Information Officers above, in addition to the following:

- Do you understand the data protection provisions of the GDPR?
- Do you know who the supervisory authorities are for all of the organization's locations and how to contact them within 72 hours in case of a breach?
- Do you understand whether your organization requires a data protection officer under the terms of the Regulation?
- Have you reviewed the responsibilities of the DPO and determined whether you could fulfill them in your current role?
- Are you prepared to filter out the legitimate requests for information from fraudulent ones intended to create data breaches? This kind of fraud is highly likely in the early days after the Regulation goes into effect.

### 3.3 Marketing management

Marketing is where the most intensive use is made of personal data. It is the principal fuel of loyalty systems, advertising, targeted promotions, data analytics and more. Your company’s Marketing Manager should be able to answer the following questions:

- Do you understand the extent to which your marketing activities make use of personally identifiable information that is within the scope of the Regulation?
- If you outsource data processing, have you reviewed your vendor contracts for compliance with the GDPR?
- Have you thought through what will be needed to comply with the GDPR without compromising your core customer outreach functions?
- Have you thought about how to implement a compliant consent process in customer-facing activities that collect or use personal information?
- Do your systems and processes support the requirement to forget personal information?
3.4 Human resources management

If you are in human resources, personell, or deal with employment issues, you should ask yourself the following questions:

- Do you directly advertise, solicit or target open positions to EU residents?
- Are you familiar with and can you name all of the systems in your organization which collect, store or make use of the personally identifiable information of employees?
- Are your existing policies regarding employee data privacy sufficient to assure compliance with the GDPR?
- Do you have explicit consent processes that explain the purposes for which the data is being collected?
- Can employees review, modify and delete their data?
- Do you have policies and processes for “forgetting” employee data, and do employees understand them?
- Do you have processes to restrict access to the data and protect it both while it’s at rest and when it’s in transit?
- Do employees understand the process for exercising their data privacy rights within your organization?
- Do you understand your organization’s responsibilities in connection with data breaches?
- Are the roles, responsibilities and contact information in place that will allow your organization to carry out those responsibilities if the need arises?
- Are your vendors compliant with the GDPR in the way that they handle employee data (e.g. for payroll purposes).

3.5 System vendors

If you provide systems, services or other goods to hospitality companies, you should ask yourself the following questions:

- Do your contractual arrangements clearly define the roles of controller and processor, and do you know where accountability lies for the data sets?
- Do your contractual arrangements clearly define the purpose, scope and limitations of processing?
- What mechanisms and controls are in place to provide for the rights of the data subject to access, amend, delete, export/transfer, restrict and object?
- Do you have a clear awareness and training program that supports the protection of personal data (e.g. organizational controls)?
- Do you have clearly communicated breach detection and breach reporting policies and processes (e.g. organisational controls)?
- What mechanisms are in place to record the capture of consent and the associated version of terms, conditions and privacy notices?
- Does functionality exist to automatically purge data after a specific period of time?
- Do you know which of your customers have operations that are within the scope of the Regulation?
- Do you understand the requirements of the GDPR as they pertain to your products and services?
- Have you reviewed model contract clauses to prepare for the obligations that your customers will be placing on you?
- Can you document compliance and demonstrate it if necessary?
- Do your engineers and installers understand the importance of protecting privacy and maintaining effective system protections?
- Do you have a mechanism for complying with a customer’s requirement to review, modify or delete individuals’ personal data?
- Do you have a dedicated security officer or team?
- What is your security strategy and how is it prioritized?
- Do you have mechanisms in place to inform data subjects when the original intended purpose of the processing changes?
- What are your policies and processes for reporting breaches to customers, authorities and data subjects?
- What third-party organizations have access to the data processed through your technology, and do you have clauses in your contracts with them that require compliance with the Regulation?
- How often do you do vulnerability scans and what do you do with the results?

### 3.6 Legal departments

If you handle legal, compliance, or risk management, you should ask yourself the following questions:

- Do you understand the GDPR’s definition of personally identifiable information well enough to recognize it within your organization?
- Is it clear who within your organization’s executive team owns the responsibility for compliance with the GDPR?
- Have you thought through the implications of the GDPR not only in terms of corporate risk management but also in terms of cross-border data discovery?
- Do you understand where data within the scope of the GDPR can be found in your organization?
- Do you understand where and how it is collected, stored and processed?
- Have you thought through which of your suppliers fall within scope, and the ways in which your contracts with them will need to be restructured?
- Do you have internal processes for the ongoing assessment of the risks associated with non-compliance?
- Are the lines of escalation clear with respect to risks that are uncovered through this process?
- Do you have processes for monitoring and assessing ongoing changes to the Regulation or to its interpretation by courts and regulators?
- Do you have processes for monitoring and assessing EU commission or EU member state clarifications or case laws that affect the GDPR?
- Do your cyber insurance contracts void your data breach protection if your company is not in compliance with the GDPR?

### 3.7 General Managers and on-property management

If you are operate and manage a hotel on a daily basis, you should ask yourself the following questions:

- Do you know every system and location on your property where personally identifiable information is transmitted, collected, stored and used? This may be in systems, on desks or in file folders.
- Do you have a Code of Conduct for handling guest data that is compliant with the requirements of the GDPR?
- Do you have an ongoing employee training program which employees must go through when they’re hired and must repeat at regular intervals afterward?
- Are data privacy and security regularly on the agenda of your staff meetings?
- Do you have processes through which guests can review, modify or delete data that you’re holding on them?
- Do you have processes for handling guests’ data erasure requests that come to your property from chains, management companies, OTAs or other channels?
- Do you know whether your systems (email, PMS, POS etc.) are up to date on their security patches? Whether the default installation passwords have been replaced and updated?
• Do you maintain auditable records so that you can demonstrate compliance to regulators and other authorities?
• Do you have compliant consent processes for data that you collect directly from guests?
• Do you understand the lawful purposes under the GDPR for collecting guest data, and are you compliant with those?
• Do you have a process for recognizing that a breach has taken place and notifying all necessary parties?
• Do you have the necessary contact information, and is your staff trained on what to do?
• Do your vendor contracts contain clauses that are compliant with the Regulation, and do your vendors have the processes and systems in place to execute against those requirements?

3.8 Franchisors and franchisees

Most often franchisors and franchisees will be joint controllers under the Regulation, meaning they jointly determine the purposes and means of processing. The GDPR requires that the roles and responsibilities with respect to the data need to be explicitly agreed to, that data subjects need to be informed of this and that the data subject may enforce his or her rights against both, either together or separately.  

Furthermore, it is likely that in many jurisdictions, franchisors will be held accountable for the lapses of their franchisees. Given this, the following concerns achieve high importance:

• Have you identified all of the personal data that you hold and use with respect to its legal basis under the Regulation? Is it lawfully held and used?
• Have you explicitly identified the flows of PII shared on both sides of the franchise relationship and how the data passes from one party to the other?
• Have you reviewed data transfer requirements under termination clauses to determine whether they are lawful under the GDPR? This is especially important when the franchisee is within the EU and the franchisor is outside of it.
• Have you reviewed your franchise agreements for compliance with the Regulation?
• Have you implemented mechanisms for jointly and separately enabling consent requirements, including:
  o informing the data subject of the purpose for the collection of data, the length of time it will be kept and his or her right to review, modify and delete it?
  o withdrawing consent?
• Have you reviewed the third-party data processing agreements used by both franchisors and franchisees for compliance?
• Have you reviewed the security status of the systems and processes involved in the management of PII? Is it current? Are there defined processes and accountabilities for keeping it current?
• Have you determined the responsibilities and accountabilities of both franchisor and franchisee in the event of a breach? Does this include actions to be taken, time frames and contact information?
• Have you determined whether either or both parties to the franchise agreement are required to appoint a data protection officer?
• Do both parties maintain auditable documentation in order to demonstrate compliance with the Regulation?

7 See Article 26: Joint Controllers
3.9 Data protection officer requirements

The General Data Protection Regulation applies broadly to organisations large and small, complex and simple. It mentions that the extent of data protection expertise required of any organisation ought to be consistent with the level of that organisation’s data processing sophistication (Rec. 97). The regulation offers recommendations of sources that data controllers and processors should turn to for compliance guidance. Notably, the GDPR suggests the designation of a data protection officer (DPO), although it acknowledges that doing so may not be universally applicable (Rec. 77).

3.9.1 When are DPOs necessary?

The regulation identifies three (3) cases that necessitate the designation of a DPO (Art. 37). The first and third apply to organisations that process data as a public authority and a law enforcement agency, respectively. The second case applies to organisations whose core activities “require regular and systematic monitoring of data subjects on a large scale.” This includes organisations that offer goods and services to EU data subjects (regardless if payment transaction is made) and/or monitor their behavior. Recital 91 can help to clarify what may be conceived of as large-scale processing operations.

3.9.2 Role of the DPO

Reporting to the executive management level, the DPO is an organisation’s personal data advocate, involved with all issues relating to the protection of personal data. Furthermore, they must have access to all aspects (e.g., nature, context, scope, purpose) of data processing; they shall not be shielded from vital details regarding the risks associated with data processing operations (Art. 39.2). In order for the DPO to satisfy their role, controllers and processors must make available all resources that he/she/they will need. Even though DPOs are designated by controllers, they do not take direction from controllers. Instead, DPOs need to enjoy independence; they must be free from any organisational conflicts of interest while performing their duties and shall not be penalised for performing tasks. (Art. 38.3).

3.9.3 Tasks of the DPO (Art. 39)

Appropriate tasks for the DPO include, but are not limited to:

- Inform and advise the controller or the processor as well as all those involved in processing activities of their obligations according to the GDPR:
  - Determine need to conduct a data protection impact assessment (DPIA)
  - Determine risk mitigation safeguards needed
- Monitor the progress of initiatives and compliance
- Assign responsibilities
- Raise awareness and train staff
- Cooperate with the EU supervisory authority
- Act as the data processing “contact point” for both supervisory authorities and individual data subjects
- Maintain a record of processing operations
- Document decisions made and actions taken (with and contrary to the DPO’s advice)

3.9.4 Expertise and professional qualities

There is no recognized, institutionalised data protection officer “certification,” and Article 37 – Designation of the data protection officer – does not specify professional qualities that DPOs must possess. However, the following are widely viewed as essential qualities for DPO candidates:

- Expertise in national and European data protection laws and practices
- Comprehension of the GDPR
- Experience in data protection program management
- Personal integrity
3.10 How can you tell how ready you are?

The HTNG GDPR Workgroup’s Self-Assessment Questionnaire will walk you through the preparedness categories. The questionnaire will help determine where you have the most work to do, and through the formulation of the questions you will be answering, it will point you toward steps to take to increase your readiness.

3.11 Conclusion

The GDPR is a major new regulatory framework with a global reach and heavy penalties for non-compliance, going into effect in May of 2018.

As with other regulations, there are areas that need to be fleshed out either through official clarifications or through test cases pursued in the courts. Nevertheless, the main provisions are clear enough that prompt action now and should reduce the likelihood of your organization becoming one of those test cases. HTNG encourages organisations to take GDPR seriously and to invest effort now to avoid adverse business impacts down the road.

It’s also important for companies to think broadly about data protection whether or not they’re subject to the GDPR. Recent incidents have shown how quickly a company’s brand reputation can be destroyed when a data breach becomes widely known, particularly when it appears that data protection wasn’t taken seriously.

However, risks and exposures aren’t the whole story either. HTNG believes the industry has a moral and ethical obligation to be a good steward of peoples’ data. Compliance with the GDPR is part of this, but it is only one part.
4 Customer Rights from a Guest Centric Point of View

4.1 Definitions

**Data Controller:** The data controller determines the purposes and means of processing personal data.

**Data Processor:** The data processor processes personal data on behalf of, and at the direction of, or under the instructions of the controller.

4.2 GDPR – Customer rights

4.2.1 The right to be informed

Guests have the right to be told what data will be held about them and what that data will be used for. In all cases, guests must be told the following:

1. Identity and contact details of the controller and the data protection officer
2. Purpose and lawful basis for processing the data
3. The legitimate interests of the controller or third-party where applicable
4. Any recipient or category of recipients of the personal data
5. Details of transfers to other countries and safeguards in place
6. Retention period
7. The existence of each data subjects’ rights
8. The right to withdraw consent at any time where relevant
9. The right to lodge a complaint with a supervisory authority
10. The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

If the data is being obtained directly from the guest, they should also be informed whether the provision of personal data is part of a statutory or contractual requirement and the possible consequences of not providing the information.

If the data is not obtained directly from the guest, the guest should be told the source of the personal data and whether that is a publicly accessible source.

In practice, this will involve explaining what the data will be used for, how long it will be kept and any other companies that the data will be shared with. In some cases, hotels will need to get permission from guests when obtaining their data if there is no other legal basis for collecting and processing it. In that scenario, hotels will need to keep track of how consent has been obtained and make it possible for guests to withdraw that consent.

Software systems (CRM, PMS, POS etc.) will also need the ability to erase data that is older than the retention period. This could be offered as a service from the vendor.
4.2.2 The right of access
Guests have the right to ask for access to their personal data free of charge in a commonly used electronic format (e.g. XML, JSON, CSV).

In practice, this means that either software systems (CRM, PMS, POS etc.) will need the ability to export data or that the vendor of the system can offer this as a service.

4.2.3 The right to rectification
Guests have the right to have their personal data rectified if it is inaccurate or incomplete. This includes informing any third-parties to whom the data has been disclosed. The request must be completed within one month (can be extended by two months for complex requests).

4.2.4 The right to erasure
The right to erasure is also known as “the right to be forgotten.” Guests can request the deletion of their personal data where there is no compelling reason to continue processing it. This isn’t an absolute right and guests can only request this in the following circumstances:

- Where the data is no longer required for the purpose for which it was originally collected
- When the guest withdraws consent
- When the guest objects to the processing of the data and there is no overriding legitimate interest for continued processing
- The personal data was unlawfully processed (i.e. it was in breach of the GDPR)
- The data has to be erased in order to comply with a legal obligation

4.2.5 The right to restrict processing
Guests have the right to block or restrict processing of data, for example, where the accuracy of the data is being questioned. This means the data controller can continue holding the data, but is not allowed to process it.

4.2.6 The right to data portability
Similar to the “right of access,” this right gives guests the right to copy or move their data from one provider to another. For example, if a guest wanted to provide a hotel chain with preference data that was being held by a competing hotel chain.

4.2.7 The right to object
Guests have the right to object to processing and profiling unless the data controller can show a compelling legitimate reason for the processing.

4.2.8 Rights relating to automated decision making and profiling
Guests have the right not to be subject to a decision when that decision is based on automated processing and it produces a legal effect on the individual.

4.2.9 Breach notification
The supervisory authority needs to be notified of a breach within 72 hours (GDPR Article 33), whereas the data subject in situations where it is likely to result in a high risk to the rights and freedom of a person, the data subject should be notified without undue delay (GDPR Article 34).
4.2.10 Accountability and governance

In order to ensure the requirements of the GDPR are being met, data controllers and processors should record all processing activity and ensure access to personal data is restricted to those who require it.

4.2.11 Legacy data

Note that the circumstance relating to unlawful processing could mean the deletion or anonymization of all historic (in scope) data in advance of the May 2018 deadline. If companies are holding personal data currently, consent for each defined purpose was not obtained for that data, and no other legal basis exists for holding that data, it will have to be deleted or anonymized. However, individual companies should evaluate their own needs and develop their own policies while managing risk appropriately. Many hotel brands have published policies that describe guest data retention options beyond the stay. Currently, there is no direct guidance from the EU commission, but an existing case law indicates that fines are possible when marketing without permission or consent.
5 Risks of Data Loss & Obligations

5.1 Power of supervising authorities to impose corrective measures

Article 58 of the GDPR delegates to the supervising authority of each EU member state the power to impose sanctions or corrective measures upon entities that do not comply with GDPR, or that present a likelihood of noncompliance. The full range of these “corrective powers” is set out in Schedule A (Section 5.5). These corrective powers range from warnings or reprimands, various orders to entities to bring their actions into compliance, to the imposition of administrative fines. Article 83 addresses the imposition of administrative fines and will be discussed further in this memorandum. On October 3, 2017, the Article 29 Working Party issued “Guidelines on the application and setting of administrative fines” to provide further detail on this topic.

A principle of the power to impose sanctions is the concept of “equivalence.” This principle stresses the obligations of the supervisory authorities to ensure consistency in their use of corrective powers generally, and in the application of administrative fines in particular. Each of the member states has equivalent powers for monitoring and ensuring compliance with GDPR, including equivalent powers for issuing fines or other sanctions. Supervisory authorities are required to cooperate to ensure the consistency of application and enforcement of the regulation.

Corrective measures should be “effective, proportionate, and dissuasive.” Corrective measures and administrative fines should adequately address the nature, gravity and consequences of the noncompliance. Supervisory authorities must assess all of the facts of the case for a sanction that is effective, proportional and dissuasive in each case to also reflect the objective of the corrective measure. The objective may be to reestablish compliance with the rules, to punish unlawful behavior, or both. Member states may pass national legislation to set additional requirements on the enforcement procedure, such as deadlines for making representations, appeal, enforcement or payment.

Administrative fines may be imposed for a wide-range of infractions and each case should be assessed individually. While administrative fines are an important tool, supervisory authorities are encouraged to use a balanced approach in their use of corrective measures in order to achieve both an effective and dissuasive, as well as a proportional action, to a compliance breach.

5.2 Imposition of administrative fines by the supervising authority

Article 83(2), attached as Schedule B (Section 5.6), provides a list of criteria the supervisory authorities are to use in the assessment of whether a fine should be imposed, and the amount of the fine, if any. Facts and circumstances considered when determining if an administrative fine should be imposed, may also be used to determine the amount of the fine. When a fine has been chosen as the appropriate corrective measure, the tiered system found in Article 83(4)-(6) is applied in order to identify the maximum fine that can be imposed according to the nature of the infringement in question. Specific infringements are not given a specific price tag, only a cap. The lowest tier of administrative fines, has a cap of €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The offenses which fall into this tier generally include the administrative requirements imposed by GDPR.

The second tier of offenses provides for administrative fines up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The offenses which fall in this tier generally pertain to violations of the rights of data subjects. Finally, noncompliance with an order by the supervisory authority pursuant to their corrective powers shall be subject to a fine up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Certain factors have been specifically identified in the Working Party’s Guidance as being important when determining the amount of an administrative fine. These factors include the number of data subjects effected and the level of damage suffered by them. The number of data subjects involved should help
identify whether the specific incident was an isolated event, or if it is symptomatic of a more systemic breach or lack of adequate routines in place.

If the data subjects have suffered damage, the level of damage has to be taken into consideration. Although this level of damage is taken into consideration, the supervising authority is not authorized to award specific compensation for the damage suffered. The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the damage. The supervising authority will also consider whether the breach was the result of willful conduct on the part of the offending controller or processor, a failure to take appropriate preventive measures or some inability to put in place the required technical and organizational measures. The supervisory authority will also consider the intentional or negligent character of the noncompliance.

The supervisory authority will consider any action taken by the controller or processor to mitigate the damage suffered by data subjects. Therefore, the offending party should do what they can to reduce the consequences of the breach for the data subjects. This will be taken into account by the supervisory authority in their choice of corrective measures, as well as the calculation of an administrative fine, should one be imposed. The entity's reaction to a breach can be a considerable aggravating or mitigating factor in the determination of the appropriate corrective measure, including the amount of any fine that may be imposed.

The supervisory authority will also take into account whether the controller or processor took appropriate steps prior to a breach. They will assess whether the entity implemented the appropriate technical, organizational and other security measures required by GDPR. Specifically, Article 25 and Article 32 of the GDPR require that controllers "take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms for the natural persons posed by the processing." In other words, the controller must make the necessary assessments and reach the appropriate conclusions regarding these requirements. Clearly, these requirements are not a one-size fits all. The supervisory authority will determine what extent the controller did what it could be expected to do given the nature, the purpose or size of the processing, in light of the obligations imposed by the GDPR. Industry standards, best practices and codes of conduct in the respective field or profession are all taken into account.

The supervisory authority will consider whether there have been any relevant previous infringements by the controller or processor, as well as the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement. Other factors to be considered are the categories of the personal data effected by the infringement and the manner in which the infringement became known to the supervisory authority. In particular, determine if the controller or processor notified the supervisory authority of the infringement, complied with any previous orders from the supervisory authority, and if they complied with Article 40 ("Codes of Conduct") and Article 42 ("Certification").

5.3 Jurisdiction for corrective measures when the data controller or processor operates in more than one member state

Although the Articles and the "Guidelines" issued by the Article 29 Working Party do not specifically address this point, Articles 60, 61 and 62, provide a framework for the supervising authorities to cooperate with each other. Article 60 introduces the concept of a lead supervisory authority, which shall cooperate with other concerned supervisory authorities to reach consensus opinions.

Article 61 provides for supervisory authorities to provide mutual assistance to each other. Article 62 requires supervisory authorities, when appropriate, to conduct joint operations "including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved." If the data controller or processor has establishments in several Member States, or there are a significant number of data subjects who are likely to be affected by the
processing operations in more than one Member State, each Member State shall have the right to participate in the joint operation.

The competent or lead supervisory authority shall be in the Member State in which the controller or processor has their "main establishment" (Article 56). The lead supervisory authority shall invite the supervisory authorities in the other Member States to take part in the joint operations.

5.4 Jurisdiction for corrective measures when the data controller or processor is not located in the EU

Once again, although the Articles of the GDPR do not specifically address this issue, the above analysis is applicable. The supervisory authority of the member state in which the non-EU data controller or processor does most of its business or has the greatest potential effect on data subjects, would be presumed to be the "lead" supervisory authority.

5.5 Schedule A

ARTICLE 58

Powers
2. Each supervisory authority shall have all of the following corrective powers:
   a. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
   b. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
   c. to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
   d. to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
   e. to order the controller to communicate a personal data breach to the data subject;
   f. to impose a temporary or definitive limitation including a ban on processing;
   g. to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
   h. to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
   i. to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
   j. to order the suspension of data flows to a recipient in a third country or to an international organisation.

5.6 Schedule B

Article 83

General conditions for imposing administrative fines
1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
3. **Administrative Fines**

   a. the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;
   
   b. the intentional or negligent character of the infringement;
   
   c. any action taken by the controller or processor to mitigate the damage suffered by data subjects;
   
   d. the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
   
   e. any relevant previous infringements by the controller or processor;
   
   f. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
   
   g. the categories of personal data affected by the infringement;
   
   h. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
   
   i. where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
   
   j. adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
   
   k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

   a. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
   
   b. the obligations of the certification body pursuant to Articles 42 and 43;
   
   c. the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

   a. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
   
   b. the data subjects’ rights pursuant to Articles 12 to 22;
   
   c. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
   
   d. any obligations pursuant to Member State law adopted under Chapter IX;
   
   e. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
5.7 Undue delay

Article 33 of the GDPR requires that in the case of a personal data breach, “[T]he controller shall without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach to the supervisory authority...unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.”

Article 34 contains similar language with regard to notification of a personal data breach to affected individuals. It states, “When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay.”

With that being said, the GDPR does not give further guidance to the meaning of the term “without undue delay.” Companies should have processes in place (including making sure one is able to contact individuals directly to avoid a public release) before a data breach which will enable you to act quickly and avoid issues with undue delay.

HTNG’s GDPR for Hospitality Workgroup strongly advises any entities subject to the GDPR to not wait until a data breach occurs to first determine how it should be investigated, and which decisions to make in regard to notification. To be proactive, all entities should have very specific procedures or processes in place, which can immediately be implemented as quickly and orderly as possible upon discovery of a data breach.

The 72-hour notification requirement does not account for holidays and weekends. HTNG believes that the 72 hour requirement does not reflect the reality of a modern data breach. Article 33, Section 3 details the minimum information which must be contained in the notification to the supervisory authority. It will be difficult for any company to compile the required information in such a short period of time. Strong consideration must be given to the caveat that notification to the supervisory authority is not required if the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. There is no further definition of “unlikely,” “risk” or “rights and freedoms.” The focus here must be on the nature of the personal data, which is the subject of the breach. HTNG’s GDPR for Hospitality Workgroup suggests that entities notify the supervisory authority within 72 hours of becoming aware of a personal data breach, even if they do not have all of the information to be included in the notification pursuant to Article 33, Section 3. The entity would then supplement the notification as soon as possible as additional information becomes available. The initial notification, with subsequent supplementation, is less likely to incur the wrath of the supervisory authority, as opposed to notifying after the 72-hour period and attempting to justify why the entity did not comply with the 72-hour requirement. GDPR recognizes not all information for notification will be known within the first 72 hours. When appropriate, notification can be done in stages.

Article 34 requires notification to the affected data subjects and does not contain the 72-hour requirement. Article 24 only states notification must be “without undue delay,” but there is no further guidance for the meaning of this term. Notification to individuals must be made only if the personal data breach is likely to result in a high risk to the rights and freedoms of the individuals. Although this requirement is stated somewhat differently than the exception for notification to the supervisory authority under Article 33, the result of reading these two requirements together is: If the personal data breach is not likely to result in a high risk to the rights and freedoms of individuals, notification is not required to the affected date of subjects. This notification to the supervisory authority can be avoided if the data breach is not likely to result in a risk to the individuals.

Article 34 explains even if the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, notification to the data subjects is not required if:

a. the data had been rendered unintelligible, i.e., encrypted; or
b. the entity has taken subsequent measures so that there is no longer a high risk to the rights and freedoms of individuals; or

c. individual notification would involve a “disproportionate effort.” (There is no definition of “disproportionate effort.”) In cases of disproportionate effort, notification should be accomplished through public communications.

Despite the lack of guidance regarding certain requirements, the group recommends data breaches should almost always be reported to the supervisory authority within 72 hours of becoming aware of the breach. If all information required is not known within this 72-hour period, a supplemental notification should be given. If notification to individuals is required, all steps taken to notify individuals should be well-documented to show the entity acted with haste and dispatch. The group recommends internal policies should reflect when personal notification is required as soon as possible, and not more than thirty (30) days after the discovery of the breach.
6 Data Transfer Across Borders and Data Governance

The travel industry is uniquely affected by regulations around international data transfer due to many travel transactions involving a transfer of data outside of the EU. Under the GDPR (and the current law), international data transfer can only happen in certain situations. The primary justifications for data transfer for travel companies will be jurisdiction-based and contract-based. There are other ways to justify international data transfer, which are more burdensome, but may be useful in situations where a contract can't be obtained.

6.1 Conditions that allow data transfer outside the EEA

Cross-border data transfers to a recipient in a third country may take place (without a need to obtain any further authorisation) if the Commission has decided the third country ensures an adequate level of data protection (an "Adequate Jurisdiction"). This principle is based on the fact that certain jurisdictions provide sufficient protection for the rights and freedoms of data subjects without the need for further safeguards. The current list of “Adequate Jurisdictions” is here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

The EU-US Privacy Shield will remain in effect after the GDPR, but will be reviewed again as soon as the GDPR goes into effect. This means Privacy Shield members are covered under the "Adequate Jurisdiction" rule.

6.2 Model clauses

A controller or processor can use model contract clauses to justify a transfer. These model clauses do not require any further authorization from any country’s Data Protection Authority (DPA).

Model clauses can be found at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

6.3 Consent

A data subject can consent to international data transfer, but the conditions for that consent are higher than other consents. The consent needs to be given through an explicit action after the data subject is informed of the risks of the transfer.

Cross-Border Data Transfer may take place if the transfer is necessary for:

   a. the performance of a contract between the data subject and the controller; or
   b. the implementation of pre-contractual measures taken in response to the data subject’s request; or
   c. the performance of a contract between the controller and a third party, where it is in the interest of the data subject.

6.4 Public interest

A cross-border data transfer may take place if the transfer is necessary for important reasons of public interest. These interests must be recognized in EU law or in the law of the member state in which the controller is located. This will likely cover airlines when they submit passenger and crew lists for security screening.
6.5 Binding corporate rules

For global companies doing inter-department transfers, a standing justification can be granted by a Data Protection Authority (DPA) based on binding corporate rules.
7 Relationship Between PII Code of Conduct and GDPR

Personally Identifiable Information (PII) is any information about an individual maintained by an organization, including any information that can be used to distinguish or trace an individual's identity.

In June of 2017, HTNG’s PII Workgroup published the “Hospitality Industry PII Code of Conduct.” This body of work is composed of four documents, the "Principals and Rationale," "Guidelines," a self-assessment tool and the "Code" itself. The code of conduct was designed to communicate to guests how companies in the hospitality industry use and protect guest data. Many guidelines associated with the code imply the same protections, offered voluntarily, now required by the GDPR. Many of the principals covered in the guidelines are essentially the same principals considered by the EU when developing the GDPR.

These principals include:

- Individuals own their own data and should have a say in how it is used.
- Adopters transparently, clearly and concisely share with people the data they hold about them and how it is being used.
- Adopters commit to be good stewards of the data they hold, protecting the data and responding to issues in a timely fashion, and with a sense of urgency.
- Adopters select partners that share their commitments to protect the data they hold.
- Adopters obey rules and regulations required by governments and other agencies on guest information.

HTNG’s PII Code of Conduct was created to make a statement by the industry on how companies protect the data provided to them by and about their customers. Companies can subscribe to the code by passing the self-assessment and advertising it to their guests. Unlike the GDPR, the code does not have penalties, fines or means of enforcement. For the most part, if your company is compliant with the GDPR, your company will also be compliant the code of conduct. The HTNG PII Code of Conduct can be found at: http://www.htng.org/page/SpecsbyProductType.
8 Guest Data Flow and GDPR Implications

The figure above is a simplified overview of guest information regarding a hotel stay as it relates to the EU’s new regulation on privacy, GDPR. The illustration is meant to trigger conversations on the subject and aims to reach a common understanding of the matter.

Although certain common flows are outlined, the roles of the **hotel**, the **brand** and other involved parties need to be assessed on a case-by-case basis.

The scope of this document is limited to the personal data in scope for the GDPR and involved in a normal hotel room reservation and stay. Therefore, the document does not address other personal information captured, processed and stored for other purposes, such as hotel employee files, payroll processing, supplier contacts, e-mail directories, although they too are subject to the GDPR.

GDPR is only applicable if at least one of three is ‘in the EU (EEA)’

a. the data subject;

b. the data controller;

c. the data processor.
A reservation is considered an agreement between the data subject and the data controller (brand, hotel, etc.). Therefore, the collection and processing of personal data necessary to make a reservation and to facilitate a hotel stay could be based on the legal ground “necessity for the performance of a contract” (Article 6(b) of the GDPR). On the basis of this assumption, there will not be a need for a hotel to require consent from the data subject. Agreements must be in place whenever personal data is transferred between data controllers and data processors (i.e. between different legal entities) and the data subject must be informed. If the receiving party (the data importer) is located outside of the EU (EEA), a legal transfer mechanism must be established. The data exporter has the obligation to inform the data subject of the transfer.

8.1 Assumptions

The assumption for this document is that the hotel is located within the EU (EEA).

The local hotel system (Property Management System - ‘PMS’) is hosted on premise and under the control of the hotel. In the case that the PMS system is provided by a systems supplier as a kind of ‘cloud service,’ the hotel needs to ensure a data processing agreement is in place, the agreement warrants the privacy of the data in scope for the GDPR and prevents visibility of the data to other customers of the systems’ supplier. The collected personal information is limited to what is necessary to create and service a reservation at the hotel.

A hotel is the main controller of guest information and the stay is the main purpose of the processing of personal information, although there can be other controllers and processors involved from the point where the data subject (the guest to be) initiates the process. A travel agency (online or traditional) is a controller on its own, parallel to the hotel. None of the above will form a joint controller set-up except in certain chain-operated scenarios where the hotel operates under the branding of a hotel chain. In these cases, the hotel and the brand may be considered joint controllers. Joint controllers need to take shared decisions on the information processed, therefore, the licensing agreement between the brand and the hotel may influence that.

An important assumption is that the legal grounds for collecting and processing the necessary data to make a hotel reservation is the fulfilment of an agreement, i.e. ‘Contractual Necessity.’

No consent is required to process a hotel reservation and stay.

However, the data captured and processed in this context needs to be limited to what is reasonably required to make a reservation and hotel stay. Retaining additional information, such as dietary information (this could be details on an F&B check), telephone numbers dialed, websites visited through the hotel’s internet connections, etc.), could require consent if another legal basis cannot be determined.

The primary territorial scope of the GDPR covers transactions within the EU and EEA member states (27/28 countries that are part of the union plus 3 non-EU EEA members). Hotels in this territory are in scope of the GDPR. Processors located outside of the union are also in scope if they act on behalf of controllers in the union. In some cases, controllers outside of the union are also in scope if they market services to customers located in the union, for instance, websites located outside of the union, but market to EU residents and process data of EU residents.

HTNG’s GDPR for Hospitality Workgroup recommends to clearly inform the data subject of what is collected, where it is stored, with whom it is shared, for how long, and more. Use transparency in practice, even if consent is not required for a standard reservation process.

8.2 Commentary to the flow-chart

The majority of the information flows from left to right, however, the main controller is the hotel and therefore is given the letter ‘A’ as an indicator. Multiple controllers may be in play from right to left, depending on the scenario.
The information in scope of Figure 1 is what is in scope for GDPR, i.e., personal information of various degrees, but also behavioural patterns (historic stays, future reservations, detailed consumption during a stay including food and beverage movies watched, telephone numbers dialed, internet addresses visited, etc.) that can be linked to a natural person (the data subject).

Card holder data, including the credit card number (PAN), expiration date, card holder name and more, is collected during the reservation and stay processes and indicated for general information on the chart. Card holder data may be collected at various points in the flow and retained on the reservation record until settlement, but the hotel may retain this data for other purposes depending on legal requirements or other fiscal obligations. Card holder data is subject to both the GDPR and PCI DSS rules (Payment Card Industry Data Security Standards).

8.3 GDPR role(s)

Figure 1 identifies potential roles as part of the booking process. Those roles are further expanded upon in the following sections.

8.3.1 Controller-A (Hotel)

One simple scenario is a guest staying at a hotel located in the union. A guest walks in or calls the hotel directly to make a reservation. The check-in, check-out and settlement is happening physically at the front desk of the same hotel. The hotel is the data controller and the data is collected and processed to fulfil a contract with the data subject (the person who is rendering the information, consuming the services and paying for the same). Many European hotels still operate to this degree. It is clear to the data subject where and to whom he/she is entrusting his/her data. This includes possibly both personal information (subject to the GDPR) and card holder information (subject to PCI DSS).

Most of the time, consent is not required in the previous situation. The desire to stay (hotel reservation) and the actual stay make up an agreement between the data subject and the controller (hotel) and the grounds for collecting and processing the required information is based on the principle of ‘contractual necessity.’

8.3.2 Controller-B (Brand)

Most of the time, chain hotels are branded and therefore identified by the guest as a brand unit rather than a locally owned, separate legal entity. This is primarily an issue if the reservation is taking place away from the hotel, i.e. via a brand’s website. In this case, it can be argued that the brand becomes a controller or a joint controller to the hotel.

The role of the brand should be assessed on a case-by-case basis. For instance, if the brand is only involved because it runs the platform (CRS and/or web site) used to collect the personal data from the customers, it is likely to be a processor.

The brand must identify another legal basis (e.g. consent) for its own use of the data where that is beyond the primary purpose, i.e. making a reservation at a hotel, but also clearly state that the data subject’s information will be handed over to a parallel controller, the hotel.

The cooperation between the hotel and the brand needs to be documented in the form of an agreement between the two controllers, ensuring they respect each other’s role and the GDPR rules on the processing of the data, and, especially the handover of data from one controller to the other controller (if considered as a joint controller).
8.3.3 Processor (CRS)
In many major hospitality companies, the CRS is separate from the brand (and typically operated by a third party). The brand, however, has no real processing role on its own, but represents a pseudo-entity or facade to whom the data subject is entrusting his/her details.

On the other hand, the CRS has no identity on its own, but is a processor.

In some situations, the CRS may exist as a legal entity on its own and merely offer white-label call center and systems functionality to the individual hotels. In other situations, the CRS will be owned by the brand and act as an internal service to brand members (franchisees or otherwise associated hotels).

In either case, the CRS will technically be a processor on behalf of either the brand or the hotel and as such in need of a data controller-processor agreement between the parties involved. If the hotel is in the EU while the CRS is outside of the EU, data transfer mechanisms should also be identified.

8.3.4 Controller-C (Distributor)
The fourth entity (third controller) on the top row of Figure 1, is the distributor, which may be more than one legal entity, i.e. will often be a ‘concentrator’ such as a GDS system (Global Distribution System) and a channel manager.

Both the GDS and the channel manager are often ‘transparent’ (such as the CRS) to the data subject, but they support the travel agencies and the OTAs with access to inventory, rates, etc. and process the reservation.

The travel agent/OTA is considered a controller, parallel to the other controllers involved. As previously mentioned, there may be more controllers involved, such as a corporate travel function in front of either of these.

When the travel agent/OTA acts as a controller, strictly collecting and processing information needed to make a reservation at a hotel, it is likely that no consent will be required. However, if the travel agent/collects the personal data for other purposes than the reservation, consent or another legal basis will be required.

Also, in this case there is the need to assess the roles of the different parties on a case-by-case basis. When a travel agent, channel manager or another individual collects information only for reserving a hotel room, they are likely to have the role of processors, while the hotel is the controller. When the travel agent or channel manager processes the information collected for purposes other than the reservation (sending marketing emails to the customer, conducting profiling, etc.), they will likely have the role of data controller.

8.3.5 Data flow
The data flow required to process a reservation is illustrated by a ‘green’ arrow from left to right. The green color indicates the data can flow without consent and without a data transfer mechanism (without data transfer restrictions being invoked). This is based on the type of data limited to what is required to fulfill the contract between the data subject and the hotel, and the assumption that the data is flowing into the EU (EEA), not out of.

The red arrows illustrate data flowing in the opposite direction, i.e. from the hotel (located within the EU (EEA), to an outside entity (possibly in a third country).

The first red arrow illustrates reservation information going from a local system to the central system. A flow that is often happening for systems synchronizing reservations from central to local and vice versa.
In other words, a reservation made local for the same hotel may often be transmitted to a CRS located in a third country.

The second red arrow illustrates reservation or stay data flowing back to a central (typically branded) guest loyalty program.

There may be numerous less transparent data transfers happening, for instance, as mentioned above, where the PMS is offered as a cloud service instead of a local, on premise system, or where data is extracted to external revenue management systems. All of these transfers represent red arrows and require legal grounds, agreements and information.

8.3.6 Agreements required

At least two agreements need to be evaluated:

- The data processing agreement between either the brand and the CRS or between the hotel and the CRS.
- An agreement between the hotel and the brand which, depending on the specific set-up, may be a controller to controller (maybe even a joint controller setup) agreement or a controller to processor agreement.

If data will be transferred from the hotel (EU/EEA based) to an entity outside the EU (EEA), the legal grounds must be established through one of multiple mechanisms in place to authorize such export of personal data:

- For the processing to be lawful under the GDPR, companies need to rely on one of the six lawful bases provided in Article 6(1) of the GDPR. In addition, the transfer of personal data outside of the European Economic Area (EEA) also needs to be supported by the legal grounds listed in Chapter V of the GDPR. In the latter case, it is the data exporter (located in the EU) who will have to identify the appropriate legal ground(s) for such transfers.

The key message here is that if a company (the hotel) transfers customers’ personal data outside of the EU, it will have to identify:

a. a basis for collecting and processing the customers’ personal data (for instance in relation to a reservation as “necessary for the performance of a contract” legal basis);

b. another legal basis for the transfer of personal data outside the EEA (among the bases listed in Chapter 5).

- Cross-border transfers outside the EEA are, in principle, prohibited unless certain specific conditions are met. A company seeking to transfer personal data outside of the EEA should rely either on:

  a. **An adequacy decision** (Article 45 GDPR): companies are allowed to transfer personal data to an adequate jurisdiction, meaning a third country that the EU Commission has recognized as ensuring an adequate level of protection. For example, if the EU-based hotel (data controller) uses an independent CRS (data processor) not based in the EU, it will have to rely on a data transfer mechanism in order to share the EU customers’ personal data with the CRS. As a first step, the hotel should assess whether the CRS is based in a country that was granted an adequacy decision by the European Commission. Or, if the CRS is based in the
US, the hotel should verify whether the CRS is certified under the privacy shield (the US adequacy decision).

b. **Another mechanism ensuring appropriate safeguards** (Article 46-47 GDPR): in the absence of an adequacy decision for the relevant third country, transfers of personal data outside the EEA can be based on:

- **Binding corporate rules** ("BCRs"): internal rules that can be adopted by a multinational group or by companies engaged in a "joint economic activity." The BCRs define the global policy with regard to transfer of personal data within those entities. The term "companies engaged in a joint economic activity" is understood as covering companies under a franchise-agreement (e.g. branded hotels). For example, when considering how to ensure the transfer of personal data between hotels of the same brand, or from hotels located in the EU to the brand located outside of the EU, the brand could put BCRs in place.

- **Standard Contractual Clauses** adopted by the European Commission or by a supervisory authority ("SCCs"): The European Commission has so far issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside of the EU and one set for the transfer to processors established outside of the EU. For example, if an EU-based hotel (data controller) uses a non-EU-based independent CRS (data processor), and the transfer cannot be based on an adequacy decision, the hotel could sign controller-to-processor SCCs with the CRS.

- Other legal bases for the transfer of personal data under the GDPR include: (a) a legally binding instrument among public bodies; (b) an approved code of conduct by the competent supervisory authority or the European Data Protection Board (the “EDPB”) and the Commission; and (c) an approved certification mechanism by an accredited certification body.

When the transfer of data cannot be based on one of the above mechanisms, the company can rely on specific derogations (Article 49 GDPR). Those specific derogations include, *inter alia*, explicit consent from the data subjects, contractual necessity and legitimate interest of the controller. The derogations must be interpreted restrictively. As a consequence, derogations should not constitute a first option for a company seeking to transfer personal data outside of the EEA.

The best approach should be to:

1. Consider whether the third country provides an adequate level of protection;
2. Determine if the level of protection in the third country is not adequate in the light of all of the circumstances surrounding a data transfer, the data controller should consider relying on other adequate safeguards (e.g., standard contractual clauses, BCRs, etc.);
3. Determine if the above is "truly not practical and/or feasible," and only if so, the data controller should consider relying on the derogations provided in Article 49 of the GDPR.

### 8.3.7 Consent

The legal grounds for collecting and processing the necessary data to make a hotel reservation is the fulfilment of an agreement, i.e. ‘Contractual Necessity,’ where the desire to make a reservation represents a contract between the data subject and the hotel. Therefore, no consent from the data subject is required to process a reservation as long as the data flows only in one direction (i.e. from left to right) and that the information processed is limited to what is required to fulfil the agreement or what is required by local legislation.

However, if information is used for other purposes beyond the agreement, consent or another basis could be required. If an OTA or a brand wants to make use of the information to support its own interests, such as marketing to the data subject, they could enroll the data subject in a loyalty program or another similar program.
If the hotel collects more data relating to rendering services in-house, it may require consent or another basis if the services or activities are not covered under the original agreement or contract.

Finally, retaining information for a longer period than implied in the agreement or required by local legislation may require consent from the data subject or another basis. This is irrespective of whether the data stays locally in the PMS system (guest history) or is transmitted back to a Central Profile system/CRM system.

8.4 Use cases/Scenarios

8.4.1 Direct booking at the hotel (or even a walk-in)

Reservation

The first point of contact can be directly to the hotel, either over the telephone to a local reservation agent or in-person at the front desk, or it can involve one of more prior instances, such as a travel agency, GDS, CRS/Brand etc. This use case addresses the direct booking at the hotel.

Pre-arrival

Hotels may want to contact the data subject prior to arrival as a courtesy message, or in the form of an online check-in message. Depending on the activity, additional information may be obtained and processed, such as dietary information, bedding, etc.

Arrival

This is the first physical contact with the data subject where payment details typically are verified and/or updated, address details collected and it is possible passport or other photo ID details are also obtained and recorded during this contact.

All required information can be obtained, recorded and processed without consent if the information is mandated by legislation in the country of the hotel. However, if the hotel collects more information than required to fulfil the agreement with the data subject, or retains the information well beyond the stay, that activity will need to be justified within the legitimate interest of the hotel and expectations of the guest or by explicit consent.

Stay

From a data collecting/processing point of view, the stay will normally generate additional information in the form of charges, such as food & beverage checks (consumed meals, drinks, etc.); telephone call tickets (such as numbers dialed); internet usage, applications used online, website addresses, in-room entertainment (such as movies watched).

If details are collected beyond what is mandated by legislation and/or required as a back-up for the charges incurred, it will need to be justified as implied by the reservation, within the legitimate interest of the hotel and expectations of the guest, or by explicit consent.

Department

Physical departure from the hotel ends the service for the implied contract.

Settlement

This may happen before the time of departure, at the time of departure or shortly thereafter. This can be in form of a direct bill or most likely the payment with a credit card.
Reporting/Follow-up

This can include a transfer of information to brand loyalty programs or to external loyalty programs of the choice of the data subject.

This can also include Level-2 charge data to credit card companies or other travel management companies for corporate card holders to enable automatic processing of expense reports. This often happens for all credit card payments as the PMS system often is unable to determine if a card is a corporate card or not.

8.4.2 Call Centre Direct (mainly voice call or e-mail)

The main difference between a hotel direct reservation is the involvement of a branded or unbranded CRS and call centre that could be located outside the EU (EEA) and trigger additional legal considerations.

In the case that the CRS and call centre is located within the EU (EEA), the legal requirements are relatively simple and straightforward. Data can flow both directions if the data subject is informed and if the type of information transmitted is only what is required to fulfil the contract between the data subject and the hotel or if the flow has another legal basis under the GDPR.

If, however the CRS and call centre are located outside of the EU (EEA) and the data is flowing in both directions, from left to right (CRS to the HOTEL) and from right to left (HOTEL to the CRS), the hotel is effectively exporting information to an entity outside of the EU (EEA). This requires one of multiple mechanisms in place to authorize such export of personal data. Please see Section 8.3.6 for required agreements.

8.4.3 Online direct via own website connected to the branded or unbranded CRS

The scenario involving a branded or unbranded website connected to a CRS system outside of the hotel is in many ways a duplication of the mentioned call centre flow and will trigger the same legal considerations depending on the location of the website and CRS versus the hotel.

8.4.4 OTA or other intermediary (including physical travel agency booking via GDS or the web)

The involvement of an intermediary, agent such as an OTA (Online Travel Agency) or a traditional, physical travel agent, can possibly complicate matters. If the party merely facilitates the minimum data required to process a reservation, i.e. fulfil the contract between the data subject and the hotel, with the data flowing from left to right only, they can do so without consent or any kind of data transfer mechanism.