htng

MOVING HOSPITALITY FORWARD

GDPR FOR HOSPITALITY

1 June 2019

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 hoteliers 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 facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

TABLE OF CONTENTS

1 Document Information

1.1 CONTRIBUTORS

Author	Company
John Bell, co-Chair	AjonTech, LLC
Daniel Johnson, co-Chair	VENZA
Finn Schulz, co-Chair	Independent Consultant
Richard Sheinis, co-Chair	Hall Booth Smith, P.C
Chris Airey	Air Angel Limited
Bill Beckler	Alice
Rebecca Boyle	Choice Hotels International
Stephen Clay	Agilysys
Chris Farrar	Exceptional Innovation
Patrick Foley	Marriott International
Charles Helleputte, Diletta De Cicco	Mayer Brown
Chris Keaton	OneTrust
Robbie Laack	Kalahari Resorts
Diane Li	JC Resorts
Thomas Linder	Infor
Jeffrey Parker	Red Lion Hotels
Mark Read	Firmdale Hotels
Bryan Steele	Jireh-Tek, Ltd.
Kris Troukens	Safe Hotels
Suzanne Ward, Prashant Dutta	AccorHotels

1.2 USEFUL RESOURCES

All HTNG best practices, software specifications, white papers and other general resources can be found at this link: 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 expected to benefit from this document include:

- 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 went into effect on May 25, 2018. At that time, it replaced the EU's earlier Data Protection Directive (1995).

The GDPR covers the processing of data from 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.

1.4.1 Privacy Regulations Around the World

Beginning, perhaps, with the European Union (EU) Data Protection Directive (1995), multiple accountability-based privacy laws have emerged with an intent to protect personal data (aka personally identifiable information) from processing activities (predominantly commercial) that put people's privacy at risk. By the time Mexico ratified its Law on the Protection of Personal Data Held by Private Parties, more than 50 countries around the globe had established privacy laws. Again, the intention of this document is to provide answers to commonly asked questions regarding privacy protection in an effort for hoteliers to align with the EU's General Data Protection Regulation. Given the GDPR's comprehensiveness, aligning to it may provide hoteliers a strong privacy management foundation. However, it is advised to consult and comply to local privacy laws as well.

2 Is the GDPR Applicable to You?

If your company or your property operates in, offers employment to, directly markets to, or offers goods and/or services to individuals who are in the European Union, 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 highly advises 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. There is also information provided on the GDPR website[1].

2.1 Provisions of the GDPR

The main provisions of the GDPR cover these areas:

- *Personal Data*: 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 directly or when combined. Some refer to Personal Data as Personally Identifiable Information (PII), but the two terms are not synonymous. Personal Data and PII may have different meanings based on your jurisdiction. For the purposes of this document, Personal Data refers to the definitional provisions of the GDPR.
- *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 if they ask.
- *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 such as 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.

2.2.1 The Data Subject

A **data subject** is any person whose personal data is being processed. Such persons may include: the customer (guests), employees, employee candidates, vendors, partners or any other real person involved. This may include contacts, e-mail senders and receivers, and other less obvious persons.

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.

Responsibilities of the data controller include:

- Understanding the nature of the data being captured and used.
- Understanding the severity of the risk to the guest (employee) should the data not be adequately protected.
- Implementing appropriate technical and organizational measures commensurate with that risk to ensure that the data is being handled as required under the Regulation.
- Similarly, implementing 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.
- Collecting and processing only the data necessary for the immediate business purpose and make it available only to those who need it.
- Working only with data processors that operate in compliance with the Regulation.
- Reviewing and updating these measures as necessary.
- Being able to demonstrate compliance with these requirements.
- Direct accountability through penalties assessed by the governing ICO

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.
- At the choice of the controller, delete or return the data at the controller's request at the end of provision of services (contract end date). Article 28.3 (g) of the GDPR specifically provisions this.
- Provide the data controller with any and all documentation necessary to demonstrate compliance with the Regulation.
- Promptly notify the data controller of any possible data breach since the controller must notify the Supervisory Authority within 72 hours of any breach being detected

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 behavior as far as their behavior 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:

- Do you understand what Personal Data is as it's defined by the GDPR?
- 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?
- Do you know who is responsible for each of those activities?
- Do you understand how personal data is being protected, or how it is failing to be protected?
- Do you understand the Regulation's concept of legal basis for data processing and where it applies in your processes, such as **consent, legal requirements, legitimate interest, and contractual necessity**? Other basis may be available but are not common in hospitality.
- 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?
- Have you analyzed the gaps that could expose you to penalties under the regulation?
- Do you have plans for remedying the gaps? Plans may include:
- Training programs for new staff along with ongoing refresher training
- Process development or modification
- Modification of vendor contracts and even (possibly) replacement of systems or service providers that create significant compliance exposures
- Do you have a documented and approved code of conduct?
- Do you have plans and processes for ongoing monitoring of compliance?
- Have you assigned your staff formal responsibilities in connection with compliance?
- 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?
- 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?

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 (CIOs)

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?
- 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? Controllers should maintain logs to audit these types of requests.
- Do you have audit logs that 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 for identifying and deleting aged or unneeded data?

3.2 Chief Information Security Officers (CISO)

As a CISO, you should be able to answer the questions pertaining to CIOs 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 DPO 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? This applies when relying on consent as the legal basis for processing data.
- Do your systems and processes support the requirement to forget personal information?

3.4 Human Resources Management

If you are in human resources, personnel, 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 explanation of 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 to 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?
- Do you follow the principle of privacy by design and default? Example evidence a supplier may provide includes data protection policies/Data Protection Impact Assessments (DPIA)/Personal Information Management System (PIMS)/Information Security Management System (ISMS)
- Are mechanisms and controls 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. organizational controls)?
- Are mechanisms in place to record how consent was obtained?
- 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 operate and manage a hotel on a daily basis, you should ask yourself the following questions:

- Do you know every business process in your property where personally identifiable information is transmitted, collected, stored and used? This may be in electronic systems, on desks or in file folders, or a combination of these.
- Do you have a Code of Conduct or Privacy Policy 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? Do you know whether the default installation passwords have been replaced and updated?
- Do you ensure proper technical and organizational measures are in place to protect personal data and to ensure accountability of its use? This includes, but is not limited to, the use of personal, identifiable, and segregated user accounts. Please see the Appendix for more technical measures.
- 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 Brand, Owned, Affiliated, Managed Hotels

When data is moved, the GDPR expects that the protections afforded to that data move with it. Most often, brands and individual hotel operators and owners will be controllers under the Regulation. A best practice is to have an agreement in place between the two organizations, recognizing each of their roles and responsibilities as controllers. However, when data is exported out of the EEA, to a country that is not deemed "adequate," legal mechanisms such as the EU-US Privacy Shield, or Standard Contract Clauses must be used.

Individual hotels, brands and management companies need to evaluate their specific circumstances to understand their role within the regulation. 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.[7]

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 hotel owner is within the EU and the brand 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:
- 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?
- 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 DPO?
- Do both parties maintain auditable documentation in order to demonstrate compliance with the Regulation?

3.9 Data Protection Officer Requirements

The General Data Protection Regulation applies broadly to organizations large and small, complex and simple. It mentions that the extent of data protection expertise required of any organization ought to be consistent with the level of that organization'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 organizations that process data as a public authority and a law enforcement agency, respectively. The second case applies to organizations whose core activities "require regular and systematic monitoring of data subjects on a large scale." This includes organizations that offer goods and services to EU data subjects (regardless if payment transaction is made) and/or monitor their behavior. Recital 91 can help 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 organization'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 organizational conflicts of interest while performing their duties and shall not be penalized 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:

- Informing and advising the controller or the processor as well as all those involved in processing activities of their obligations according to the GDPR:
- Determining if there is a need to conduct a data protection impact assessment (DPIA)
- Determining if any risk mitigation safeguards are needed
- Monitoring the progress of initiatives and compliance
- Assigning responsibilities
- Raising awareness and training staff
- Cooperating with the EU supervisory authority
- Acting as the data processing "contact point" for both supervisory authorities and individual data subjects
- Maintaining a record of processing operations
- Documenting decisions made and actions taken (with and contrary to the DPO's advice)

3.9.4 Expertise and Professional Qualities

There is no recognized, institutionalized 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 GDPR Prioritized Approach

The HTNG GDPR Prioritized Approach Summary 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.

The HTNG GDPR Workgroup's Self-Assessment consists of prompts designed to provide organizations an approximation of their GDPR compliance status. The assessment is built around an ordered framework of the most pressing concerns, a 12-Step Prioritized Approach:

- Process Registry of Data: Mapped and Inventoried
- Assessments Completed and Documented
- Roles Assignments Defined
- Legacy Data Risk Assessed and Cessation of Unlawful Processes Documented
- Policies Assessed and Published
- Rights Response Procedures Formulated and Response Plan Documented
- Data Breach Procedures Formulated and Response Plan Documented
- Purge Procedures Defined
- Protection of Personal Data Measures Defined
- Agreements Assessed
- Rules of Email Use Formulated and Documented
- Training and Awareness Program Conducted and Documented

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.

3.11 Conclusion

The GDPR is a major regulatory framework with a global reach and heavy penalties for non-compliance.

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 organizations 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 Employee Data Considerations

In the hospitality industry, it is easy to focus on the personal data of guests when it comes to GDPR compliance. However, we should not allow this focus to cause us to lose sight of the bigger picture, which is that the GDPR applies to any identified or identifiable natural person. This would include hotel employees, job applicants or recruiting, non-overnight guests who nevertheless use hotel services, vendor personnel, event attendees, individuals on security camera video, and even the person who accesses the hotel's free Wi-Fi while waiting in the lobby. All requirements of the GDPR apply to these individuals, just as much as they apply to hotel guests.

GDPR compliance regarding the personal data of non-guests may present challenges that are different than compliance regarding guest personal data. The personal data of employees also deserves special attention because the GDPR allows Member States to adopt their own specific regulations regarding the protection, handling and use of this data. Each type of data also needs its own retention period.

The point is simply that while guest personal data might be our first concern under GDPR, GDPR itself makes no distinction between personal data of guests, and personal data of others for which an entity is a data controller or data processor.

4.1 The Legal Basis for Processing the Personal Data of Employees

In the employment context, the personal data of employees is, of course, subject to protection under the GDPR. Although an employee can consent to the processing of their personal data by their employer, due to the unequal negotiation power in the employer/employment context, obtaining valid consent from employees can be problematic. Therefore, relying on consent as the legal basis to process employee personal data is generally not recommended.

In the absence of voluntary consent, the employer's "legitimate interest" is the legal basis most often relied upon for processing employee data. Keep in mind, however, that an employer cannot simply state that they are processing employee data in the employer's legitimate interest. The employer must first go through the legitimate interest balancing test set forth earlier in this memorandum. Possible situations in which a legitimate interest could be used are extremely broad, ranging from background checks and security vetting in recruitment and HR functions, office access and operation, professional learning and development administration, travel administration, time recording and reporting, to processing family members' data in the context of HR records. However, legitimate interest should not be used "carte blanche."

If there is an employment contract in place, the employer can consider using the contractual necessity or legal obligation as a legal basis for the processing. While these grounds can be helpful to the employer, limitations such as the purpose limitation and data minimization principles will apply.

Lastly, employers must keep an eye on rules adopted by EU member states regarding the processing of employee data. Article 88 of the GDPR provides that EU member states may adopt more specific rules with regard to the processing of employee data. Germany, for instance, has already passed its GDPR-compliant national data protection law, which sets forth stricter requirements for monitoring employees in the workplace.

5 Data Subject Rights from a Guest-Centric Point of View

5.1 Definitions

Within the Charter of Fundamental Rights of the European Union as well as the Treaty on the Functioning of the European Union, Articles 8.1 and 16.1 respectively, the right to protect one's personal data is deemed to be fundamental to all persons. The processing of personal data, therefore, is taken seriously. Those involved in the processing of personal data have defined roles and are responsible to honor the rights of data subjects.

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.

5.2 Customer rights

5.2.1 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:

- Identity and contact details of the controller and the data protection officer
- Purpose and lawful basis for processing the data
- The legitimate interests of the controller or third-party where applicable
- Any recipient or category of recipients of the personal data
- Details of transfers to other countries and safeguards in place
- Retention period
- The existence of each data subjects' rights
- The right to withdraw consent at any time where relevant
- The right to lodge a complaint with a supervisory authority
- 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 it 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 older than the retention period. This could be offered as a service from the vendor.

5.2.2 The Right of Access

Guests have the right to ask for access, however, this can be a screen shot or very simple delivery mechanism.

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.

5.2.3 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).

5.2.4 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 when 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:

- When 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

5.2.5 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.

5.2.6 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. This right of portability applies if processing is based on “Consent” or “Contract,” as opposed to “Legitimate Interest” or other legal basis for processing.

5.2.7 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.

5.2.8 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.

5.2.9 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).

5.2.10 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.

5.2.11 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 retainment 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.

5.3 Assessing the Validity of Consent

When consent is the legal basis to process personal data, the consent is only valid if it is it “freely” given. Article 4(11). In assessing whether consent is freely given, utmost consideration must be given to whether the provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that service. Article 7.4. “Consent should not be regarded as freely given if the data subject has no genuine or free choice…” Recital 42. The UK’s Information Commissioner’s Office has specifically addressed the validity of incentivizing consent. It has stated, “It may still be possible to incentivize consent to some extent. There will usually be some benefit to consent to processing. For example, if joining the retailer’s loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who do not sign up does not amount to a detriment for refusal. However, you must be careful not cross the line and unfairly penalize those who refuse consent.” UK ICO, “Consultation: GDPR Consent Guidance”. It should be noted that incentivizing consent, is different than penalizing a data subject for refusal to consent. It should also be noted that conditioning the provision of a good or service on the data subject providing consent is not permissible. For instance, stating that a person can only join a loyalty program, and receive a financial incentive, if the data subject also consents to receive marketing e-mails, would result in the consent to receive marketing e-mails being invalid.

6 Risks of Data Loss & Obligations

6.1 Supervisory Authorities and 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 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.

6.2 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 offensives 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”).

6.3 Jurisdiction Considerations for Multi-State Issues

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.

6.4 Non-EU Jurisdiction

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.

6.5 Schedule A

ARTICLE 58

Powers

Each supervisory authority shall have all of the following corrective powers:

1. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
2. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
3. 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;
4. 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;
5. to order the controller to communicate a personal data breach to the data subject;
6. to impose a temporary or definitive limitation including a ban on processing;
7. 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;
8. 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;
9. 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;
10. to order the suspension of data flows to a recipient in a third country or to an international organization.

6.6 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:
   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 organizational 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 organization 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.

6.7 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 notifications. 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 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:

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

7 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, 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.

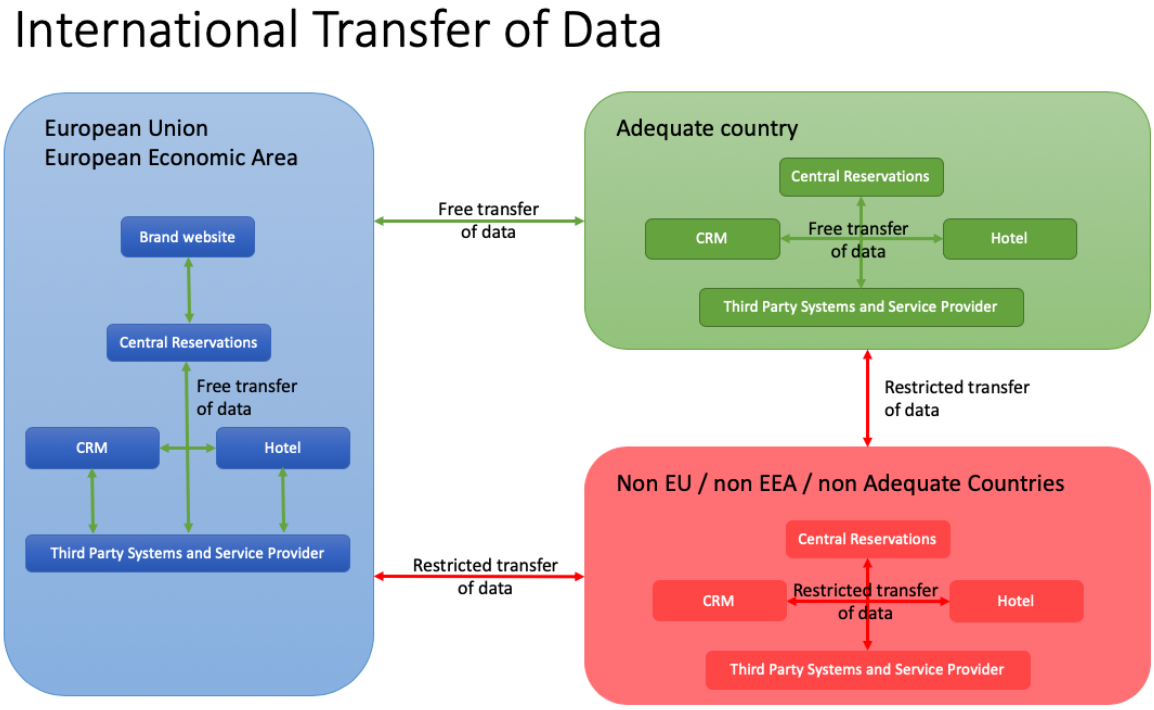

Figure 1 International Transfer of Data

7.1 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 authorization) 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" can be found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Otherwise, EU-US Privacy Shield, binding corporate rules, standard contract clauses should be used.

7.2 Adequacy Decision

The transfer may legally take place if the European Commission has decided that the third country to which the personal data is to be transferred ensures an adequate level of protection for the personal data. This is referred to as an "adequacy decision". Currently, there are only 11 countries for which the Commission has made an adequacy decision. These countries are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.

If the personal data is being transferred from the EU to one of these locations, the transfer is legal under the GDPR, and nothing further needs to be done.

7.3 Appropriate Safeguards

In the absence of an adequacy decision, personal data may be transferred to a third country if the controller or processor has otherwise provided appropriate safeguards for the protection of the data in the third country. *Article 46* sets forth the various safeguards which can be put in place to satisfy the requirement for adequate safeguards.

The most common of these safeguards is a set of contractual terms called the "standard contract causes" (the “SCC”) or the "model clauses". The SCC are a set of contractual clauses entered into by the "data exporter", and the entity located in the third country to which the data is being transferred, known as the “data importer”. The SCC currently in effect were published by the European Commission under the Directive. These SCC are still in effect, although they may be altered at some point under the GDPR.

Many of the clauses within the SCC are similar, if not identical, to the contract clauses required between a data controller and a data processor pursuant to *Article 28* regardless of the location of the controller and processor. Care should be taken, however, to note that the requirements of *Article 28* and the standard contract clauses are not completely identical, and one should not be viewed a replacement for the other. That having been said, if an entity is entering into both *Article 28* clauses and the SCC, if a clause is in one document, it does not necessarily need to be repeated in the other document.

7.4 Derogations for Specific Situations

Article 49 sets forth certain situations which allow for the transfer of personal data to a third country that is not the subject of an adequacy decision. One such specific situation is if the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards. In the hospitality context especially, obtaining such explicit consent would seem to be logistically quite difficult, and is not favored.

7.5 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

7.6 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:

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

7.7 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.

7.8 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.

7.9 Data Transfer Examples

7.9.1 European Union to United States

A hospitality entity in the EU transfers personal data to an entity within its enterprise in the U.S. The entity in the U.S. then transfers the personal data to a third entity within its enterprise, which is located in India. If the EU entity and the U.S. entity have entered into SCC, does anything further need to be done for the transfer of personal data from the U.S. entity to the entity in India to be legal under the GDPR?

The transfer of the personal data from the U.S. to India is legal only if one of the "conditions" for the transfer of data exist between the U.S. entity and the entity in India. Article 44 on the "General Principle for Transfers" states that the transfer of personal data to a third country shall only take place if the "conditions" are complied with, "including for onward transfers of personal data from the third country…to another third country."

- The EU-US Privacy Shield or a contract incorporating the Standard Contract Clauses should be in place for the transfer of the data from the EU to the USA. The same arrangement should be in place for any onward transfer of data to other legal entities within the USA.
- A contract incorporating the Standard Contract Clauses should be in place for the transfer of the data from the USA to the India. The same arrangement should be in place for any onward transfer of data to other legal entities within India.

7.9.2 Downstream Systems

A hospitality entity in the EU transfers personal data to an entity within its enterprise in the U.S. The entity in the U.S. then transfers the personal data to a third entity within its enterprise, which is also located in the U.S. If the EU entity and the first U.S. entity have entered into SCC, does anything further need to be done for the transfer of personal data from the first U.S. entity to the second U.S. entity to be legal under the GDPR?

- The EU-US Privacy Shield or a contract incorporating the Standard Contract Clauses should be in place for the transfer of the data from the EU to the USA.

The EU-US Privacy Shield or a contract incorporating the Standard Contract Clauses should be in place for the transfer of the data to other legal entities within the USA. E.g. to franchisees, or third-party systems or service providers.

7.10 Practical Application

In the absence of an adequacy decision it seems the most favored mechanism, and logistically the easiest to employ, is the use of the SCC. When personal data is being transferred from the EU to an entity in a third country and going no further the use of one of the aforementioned mechanisms is fairly straightforward. However, in hospitality there are instances when personal data might be transferred out of the EU, only to then be transferred to a second or third entity within the hospitality enterprise e.g. A franchisee, or a third party systems or services provider (Data Processor). In such cases, suitable legal and contractual arrangements should be in place between the parties sharing the data.

7.11 Legal Basis for Processing Data

The processing of personal data is only legal if there is a legal justification for the processing. Article 6 of GDPR sets out six legal justifications for the processing of personal data. Only four of these justifications will generally be applicable to the operations of a hotel. These justifications are:

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes. Article 6.1 (a).
2. Processing is necessary for the performance of a contract to which the data subject is a party or an order to take steps at the request of the data subject prior to entering into a contract. Article 6.1 (b).
3. Processing is necessary to comply with regulations. Article 6.1 (c).
4. Processing is necessary on the basis of vital interest to protect the well-being of a living individual. Article 6.1 (d).
5. Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overwritten by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child. A legitimate interest assessment (LIA) must be completed to utilize this legal justification. Article 6.1 (f).

This memorandum will strictly address the application of these legal justifications for processing personal data.

1. Processing is necessary for the performance of a contract to which the data subject is a party or an order to take steps at the request of the data subject prior to entering into a contract. Article 6.1 (b).

This legal justification for processing personal data is frequently called "contractual necessity." The data controller cannot perform the contract requested, or provide the goods or services, without processing the data subject's personal data. An example would be a data subject who wishes to make a reservation at a hotel. The reservation cannot be provided unless the hotel processes the data subject's personal data. The hotel should be careful that when personal data is processed for the purpose of fulfilling a contract or providing a good or service, the personal data is not used for any purpose other than fulfilling the contract or providing the service. While a hotel must process a data subject's personal data to fulfil a reservation, the hotel may not process the personal data for any purpose other than to fulfil the reservation. If the hotel wishes to use the data subject's personal data to also send marketing e-mails, such processing would not be lawful as a contractual necessity. Since this additional use of personal data is not necessary for providing the reservation, the hotel would need to obtain the data subject's consent to send marketing e-mails.

2. The data subject has given consent to the processing of his or her personal data for one of more specific purposes. *Article 6.1 (a).*

Consent is most often the legal justification used for marketing communications. Consent of the data subject means, any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. *Article 4(11)*.

3. Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overwritten by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child. *Article 6.1 (f)*.

Contractual necessity and consent will be the mechanisms used for the lawful processing of personal data in most instances. The circumstances under which "legitimate interest" will apply, are not as clear as the application of "consent" and "contractual necessity". The legitimate interest of a controller could exist,

"where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller." Recital 47. Under legitimate interest, special consideration must be given to whether a data subject should reasonably expect in the context of the collection of the personal data that processing for that purpose may take place.

GDPR cites three general examples of when "legitimate interest" will justify data processing.

1. There is a relevant and appropriate relationship between the data subject and the controller. An example of such a relationship is when the data subject is a client of, or in the service of, the controller.
2. The processing of personal data is necessary for the purposes of preventing fraud.
3. The processing of personal data is for a direct marketing purpose.

The direct marketing example of "legitimate interest" might sound like it conflicts with our usual understanding that consent is required to send marketing communications, legitimate interest serves as an alternative to consent only under certain circumstances. Prior to using legitimate interest as a justification for direct marketing, the data controller must consider whether a data subject should reasonably expect in the context of the collection of the personal data that processing for that purpose may take place. This is a balancing of the interest of the data controller and the data subject. If a data subject objects to receiving direct marketing, the data controller must stop sending such communications.

Although the Article 29 Working Party has not issued guidance to help us further understand legitimate interest under GDPR, the Working Party previously issued guidance on legitimate interest under GDPR's predecessor, Directive 95/46/EC. The definition of legitimate interest under the Directive was very similar to the definition under GDPR. Therefore, the guidance issued under the Directive is still instructive in helping us understand legitimate interest under GDPR.

Legitimate interest as a justification for processing personal data requires balancing of several factors, including:

- The nature of the data controller's legitimate interest
- The impact on the data subject and their reasonable expectations about what will happen to their data, as well as the natures of the data and how they are processed
- Additional safeguards which could limit undue impact on the data subject

The UK's Information Commissioner's Office has also issued useful guidance on using legitimate interest under GDPR. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. The ICO provides a three (3) part test to determine if legitimate interest is a lawful basis for processing:

- Purpose test: are you pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

It is interesting to note that the guidance issued under the Directive includes "conventional direct marketing and other forms of marketing or advertisement" as a context in which the issue of legitimate interest may arise. The guidance provides two (2) examples, which are useful to demonstrate when legitimate interest may justify data processing, and when it does not:

SCENARIO 1

A data subject orders a pizza via a mobile app on her phone. Her address and credit card details are stored for the delivery. A few days later the data subject receives discount coupons for similar products from the pizza restaurant via regular mail.

The pizza restaurant's processing of the data subject's data to send the discount coupons is permitted under the legitimate interest justification. The restaurant has a legitimate interest to sell more pizza. There is not a significant intrusion on the data subject's privacy, or any undue impact on her rights and interests. The data and context are relatively innocent (consumption of pizza). The restaurant used limited information. On balance, the interests and rights of the data subject do not appear to override the legitimate interests of the pizza restaurant to carry out this minimal amount of data processing. (It should be noted that in this scenario the pizza restaurant had an "opt out" of marketing box on its mobile app, which the data subject did not check. Under GDPR, there would be an "opt in" box, rather than an "opt out" box. We must consider how the analysis might change if the data subject did not tick the "opt in" box.)

SCENARIO 2

The same context as Scenario 1, except the pizza restaurant uses the data subject's purchase history for the past three (3) years, combines the data with data received from other sources, and starts sending her advertisements and special offers by regular mail, email and online ads, including pop-up ads on her mobile phone. In this case, the marketing would not be justified under legitimate interest. The data subject would not expect her data to be used in this manner. The marketing goes beyond what is reasonable based on the data subject's interaction with the pizza restaurant. (It should be noted that the example provided in the guidance is somewhat longer, and has additional facts, but it has been shortened for the purpose of this memorandum.)

8 Data Classifications

Article 1 of the GDPR defines a data subject or “natural person” as “one who can be identified” and provides a list of things that serve as examples of how a person may be identified including names, id numbers, locations, and social identities. Personal Data is defined in this same section as any information relating to the identified person.

Article 9 of the GDPR prohibits the processing of personal data that reveals a person’s race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also does not allow processing of genetic or biometric data for identification or data concerning health or a person's sex life or sexual orientation for the purposes of identifying that individual.

GDPR calls this type of information “sensitive data”, but in a broader business context sensitive data may include additional information such as the time, date and location where a guest may be found, even though it is not explicitly called out.

The GDPR provides examples of “sensitive” data but these examples do not include information such as reservations which reveal the time a person will be at a particular location. This is sensitive information, normal for a reservation, that needs to be protected.

Front desk personnel need awareness of these issues. For example, if someone comes to the front desk and asks if a specific guest has arrived, answering the question is a violation of the guest’s privacy.

8.1 Special Cases

- Health data may apply to allergies
- Data about minors & children (the definition of a minor or child may vary between jurisdictions)
- Social media data may be 13 years old and over (Generally, 16 years old is the threshold)
- Criminal convictions

Hospitality companies should be aware that the data examples listed below may be in several systems (CRS, GDS, E-mail, PMS and potentially hundreds of others at a single hotel). Further, if you have relationships with OTAs, or other services that feed data to you, you should have an agreement in place to govern that data exchange and how to handle guest rights invocation.

8.2 Personal Data

Personal data, in the context of the hospitality industry, includes:

- Identifying data
- Reservation data
- Customer preferences
- Payment information
- Previous purchase history
- Membership (loyalty) numbers
- Guest name & title
- Number of children and ages
- Accompanying guest name(s)
- Email address
- Phone number
- Fax number
- Nationality
- Residential address

- Loyalty membership number, level & expiration date
- Company details (company name, ID number, address, phone number, contact name, email address)
- Credit card number, expiry date and cardholder name
- Employer data
- Wi-Fi: Hardware, MAC address, etc.
- Personal Identification details, such as a copy of your Government issued ID Card or Passport.

Back-up documentation in connection with charges occurred during your stay, such as:

- Restaurant checks
- Call details on telephone calls from your guest room phone
- Sites visited using the Internet connection from your room or using Wi-Fi in the hotels
- Biometric data, such as digital images
- Images and video and audio data via security cameras located in public areas, such as hallways and lobbies
- Guest preferences and personalized data ('Personal Preferences'), such as interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit
- Historic stay details
- Consent details

Sensitive Data, in the context of the hospitality industry, includes:

- CCTV, security cameras (may be out of scope if not used for identification purposes, or if there is public notice stating that the area is being surveilled)
- Staff areas need special consideration, and a clear demonstrated need must be presented to use this information
- Facial recognition (and other biometric data collected for the purposes of identifying an individual) is sensitive data, such as part of a check-in process
- Dietary or allergy data, include food allergies or substance allergies
- Union membership for staff, unless it is required as part of the employment process (union dues, etc.)
- Health data (guest requests wheelchair accessible room)

8.3 Exceptions

Exceptions to sensitive or personal data processing prohibitions include:

- Vital interest
- Consent
- Contractual obligations

If the data is not required for contractual purposes, and the guest does not provide consent, the only acceptable reason to process sensitive data is for the vital interest of the guest (data subject).

8.4 Guest Wi-Fi, Bluetooth and Connectivity at Hotels Details

When it comes to offering guests connectivity solutions via Bluetooth or Wi-Fi, it's important to determine the role of the Venue Operator as either the Data Controller, Processor, or Sub-Processor, as this determines the format of the Data Processing Agreements that are required under GDPR.

Hotels often offer Wireless Internet Access to resident guests and other visitors. For several reasons, most Wi-Fi guest networks require identification and authentication before the service can be utilized.

Such authentication is often done via a local login page where the user (the guest) is asked to enter his/her e-mail address or room number along with a personal password and an acknowledgement of the Terms and Conditions for use of the service.

Some hotels offer the Wi-Fi service on their own, others have contracted a third-party operator to provide the network service, the authentication, etc. The question then is which 'GDPR role' has the hotel and which role has the network provider?

Typically, the hotel will be the data controller as the connection takes place in the hotel premises, often even from a guest room that said, the login screen presented to the guest can of course be clearly branded with the name and logo of the network operator and clearly stating that they guest is about to use a third-party service with its own identity and privacy policy.

In the first case, i.e. where the hotel assumes the role of Data Controller, the hotel needs to ensure a Data Processing Agreement is in place with the network service provider and the hotel should include the service in its own posted privacy policy. Use of the captured data is then subject to that Privacy Policy (scenario 'A' below).

Alternatively, if the hotel contracts the service from a third-party network operator who wants to have its own identity and often offers additional services, such as roaming access across venues or offer hardware reauthentication on repeat visits, it must be very clear to the guest that he/she is about to offer a third-party service under its own privacy policy. The identity of the network operator (Data Controller) must be clearly mentioned in the posted privacy policy including the purpose of processing and more. (Scenario 'B' below).

In the latter, it is advisable to have a data sharing agreement in place between the two data controllers, i.e. the Hotel and the Network Operator, clearly outlining the rules of operating, who is responsible in case of a breach, will the two compensate each other in case of a penalty, etc.

In case the objective of capturing user data is direct communication, the login screen must clearly state the purpose and request explicit consent. Good practice is to allow the user access to Wi-Fi even without consenting to marketing communications.

Depending on the requirements of the hotel, the login may be open for all, i.e. any e-mail address will suffice, alternatively, hotels like to limit the service to resident guests hence the connection to PMS where the authentication will include the room number along with the name or e-mail address.

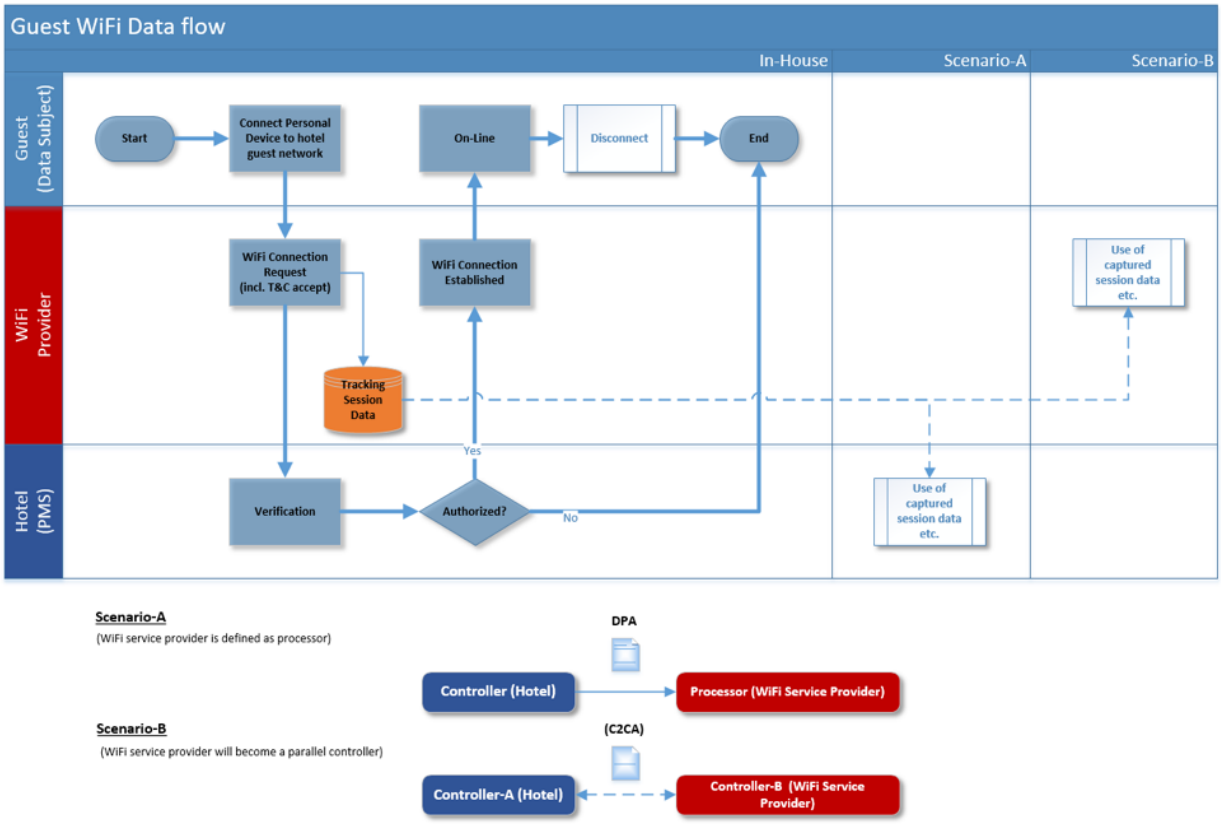

Figure 2 Guest Wi-Fi Data Flow

These relationships must be clearly specified in the sign-up terms and conditions and privacy notice, and dependent upon use, may require explicit consent from the data subject. Irrespective, it is both the Venue Operator and the Wi-Fi providers responsibility to ensure that each entity has the legal right to store & process the guest data. Without an agreement in place, neither should be processing that data.

9 Data Retention and GDPR

Article 5 paragraph (e) of the GDPR states:

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

This expresses the principal of "Data Minimization" that is expected to be followed. The direction here is to keep as little data as is needed for as short a period of time as is practical.

9.1 Data Retention Policy

Every company should have a data retention policy; however, GDPR through recital 39 practically requires it by stating that "time limits should be established by the controller for erasure or for a periodic review".

In general, a retention policy should include:

- The types or categories of data applicable to the policy
- The purpose of the data and why the data is being processed
- The events that determine the data is no longer required for processing; for example, the stay has been completed and the government mandated retention time has passed.
- The period of time the data should be retained
- The compliance strategy; for example, data deletion, anonymization, etc.
- The person or group responsible for the data and carrying out the policy
- Other rules, laws, or practices to be considered
- Conditions when certain data should be excluded from the policy; for example, if the data is part of a legal action
- Other processors that may typically be provided with the data

9.2 Data Destruction

When data is no longer needed it must be securely destroyed. This may not be as easy as it sounds. Physical media like paper should be shredded. Some data may be unintentionally left behind, for example connections between personal devices and smart televisions may leave personal information intact on the television. The same may hold true for networking equipment. Data destruction requirements include purging data from backups, including full, incremental and other types of backup processes.

The regulations imply that a record of the destruction must be maintained. In turn, this implies a shredding log for paper. It also means that as information is deleted from processing systems, a log of the deletion needs to be maintained. It is not clear whether it is necessary to securely delete the data from the storage medium using techniques such as multiple overwrites with random bits.

An alternative to destruction is to make the data anonymous by breaking the binding between the subject's identity and the rest of the information. If the data is anonymous and can't be associated with a data subject it falls out of the categories protected by the GDPR.

9.3 Anonymization and Pseudonymization

As stated in Recital 26, information that cannot reasonably be associated with a data subject or individual is not covered under the GDPR and does not require any special protection. Be careful of the "data cannot reasonably be associated with a data subject." To give an example; assume that a database has been created to track the purchases of visitors by region defined by postal code and a particular region has a single visitor. If there exists another separate database with visitor names and addresses including the postal code, it is possible with the addition of that data to associate those purchases to the individual. This is a simple example but there are a number of data points that can potentially be combined to de-anonymize information.

9.3.1 Pseudonymization

The GDPR encourages the concept and use of pseudonymization defined as;

"The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

Recital 26 clarifies that pseudo-anonymized data should be considered identifiable data and must be protected. In other passages the technique is seen as a means of protecting data by separating identifying information from other personal data.

Recital 28 suggests that pseudonymization is a good means for processors and controllers to meet their data protection responsibilities and reduce the risks to data subjects.

Recital 29 allows the use of this pseudonymized data for analytics as long as the personal data remains within the same controller and the identifying data is stored separately.

10 Audit Procedures

Most organizations will be familiar with auditing best-practices, and how best to objectively measure systems & processes against requirements, and the extent to which those systems are current, cohesive and consistent.

With the introduction of GDPR Article 5(2) there is an explicit requirement to be able to demonstrate compliance with the six core principles relating to processing of personal data. Through the use of audits, an organization should be in a position to evidence a Privacy Compliance framework and an organizational approach that puts data subject privacy at the heart of the system and process design on an ongoing basis.

Having a structured audit program and associated records of findings will assist in proving that a culture of compliance with the 'Six Principles' is in place and under continual review.

The following are examples of Audit topics to include in a schedule but are by no means exhaustive. Operators should carry out their own review of methods of providing proof of compliance, based on their own data processing environment.

10.1 Lawful, fair and transparent processing

1. Check that the Data Asset Register is being updated and reviewed to ensure there is a clear record of the lawful reason for processing.
2. Check records of Data Protection Impact Assessments, when changing processes or systems, and confirm they highlight any risks and subsequent risk treatment.
3. Confirm the Data subject is being informed as to the extent and purpose of processing. Typically, this is achieved through the presentation of a Privacy Notice.

10.2 Processing for specified, explicit and legitimate purposes

1. Carry out validation checks to confirm that data is only being used for the purposes as specified within privacy notice.
2. Confirm the legal basis is documented and that only the required data is being processed.
3. Confirm that Privacy Notices are being reviewed after any change in processing (typically identified through Data Protection Impact Assessment records).
4. At each audit, choose a different dataset, to ensure all data sets are reviewed over time.

10.3 Adequate, relevant and limited

1. Check that the retention period for the personal data storage is limited to a "strict minimum" and that the period is justifiable for each data set.
2. Check that the organization can evidence that the data being processed is limited to the minimum amount necessary for each stated purpose and that the purpose for processing could not reasonably be fulfilled by other means.
3. If any third parties have access to the data, is there an appropriate contractual agreement in place that ensures any third-party processing is carried out in line with the Data Controllers requirements? This may involve auditing of supplier processors.

10.4 Accurate and maintained up-to-date

1. Review the organizational processes that are in place to ensure data is kept up-to-date
2. Confirm records can be amended by either the data subject using a "self-serve" portal or that there is a clear process for rectification, deletion and export, as per the Data Subjects rights.

3. Review the Subject Access Request (SAR) Policy and Process is in place and is in use consistently across the organization.

10.5 Kept for no longer than necessary

1. Query data records for any data stored beyond the retention period stated within the Privacy Notice
2. Confirm that there is evidence of a data-minimization process (this can include deletion, anonymization & pseudonymization)

10.6 Processed in a manner that ensures appropriate security

1. Does the organization have a formal or recognized Information Security Management System or framework, such as ISO27001, Cyber Essentials or similar that minimize the risk to the confidentiality, integrity and availability of the personal data?
2. Can the relevant departments demonstrate that the data is protected when the data is “At Rest”, “In Transit” and “In Use” for active systems and processes?
3. For any cross-border data transfers, what measures are in place to ensure compliance (a-typically through adequacy, contractual clauses or binding corporate rules)?
4. Has the organization implemented a segregation of duties, access control lists (using the “least privilege” method), to minimize the risk of accidental or malicious loss, destruction or damage of the data?
5. What Data Loss Prevention controls are in place (such as the encryption of mobile device hard drives and password policy enforcement)?
6. Confirm that a Backup & Recovery Process is in place and that this is tested on a regular basis
7. How can the organization demonstrate that there is a breach response and notification plan in place that ensures the requirement to notify the relevant Supervisory Authority within the 72h deadline, and that the Data Subjects will be notified where required?

11 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 with the code of conduct. The HTNG PII Code of Conduct can be found at: http://www.htng.org/page/SpecsbyProductType.

12 Guest Data Flow and GDPR Implications

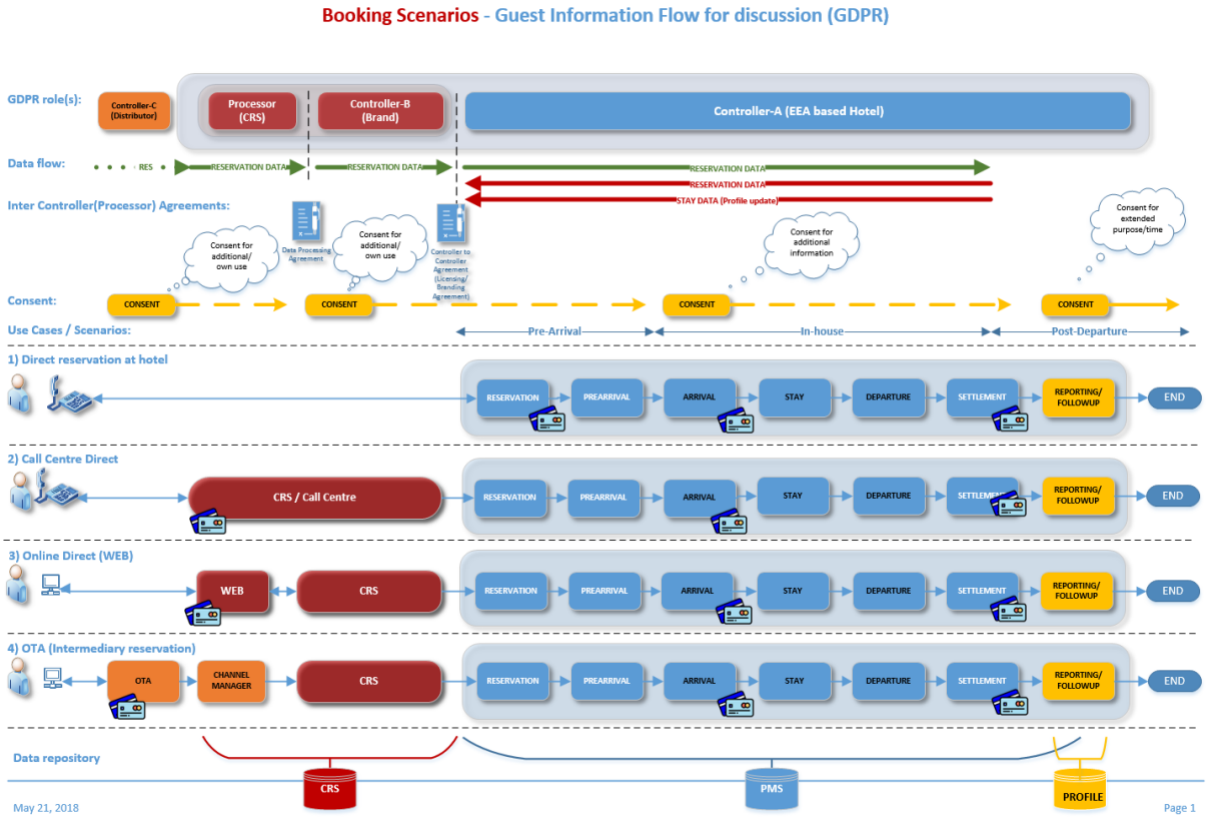

Figure 3 Booking Scenarios

The above flow is a simplified overview of the guest information regarding a hotel stay as it relates to the EU Regulation on privacy (GDPR).

The illustration and assumptions are meant to trigger debate on the subject and hopefully reach a common understanding of the matter.

Although we outline certain common flows, 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 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, for instance hotel employee files, payroll processing, supplier contacts, e-mail directories etc. although they too are subject to the GDPR.

GDPR is only applicable if at least one of three is ‘in the EU (EEA)’ (i) the Data Subject; (ii) the Data Controller; or (iii) 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) GDPR). On the basis of this assumption, there will be no need for an 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 the EU (EEA) a legal transfer mechanism must be established. The Data Exporter has the obligation to inform the Data Subject of the transfer.

12.1 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 case 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 and that the agreement ensures the privacy of the data in scope for GDPR and prevents visibility of such 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.

The consensus is that the HOTEL is the main CONTROLLER of the guest information, as 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) is initiating the process. A Travel Agency (online or traditional) would be a CONTROLLER on its own, parallel to the hotel. It is generally understood that none of the above will form a kind of JOINT CONTROLLER set-up except in certain chain-operated scenarios where the hotel operates under a branding of a hotel chain. In such cases the HOTEL and the BRAND may be considered Joint Controllers. Joint Controllers need to jointly take 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 that context needs to be limited to what is reasonably required to make such a reservation and hotel stay. Retaining additional information such as dietary information (could be details on an F&B check), telephone numbers dialled, websites visited via the hotel's internet connections, etc.) could require consent if another legal basis cannot be determined.

The primary territorial scope of the GDPR Regulation 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 GDPR. Processors located outside the UNION are also in scope if they act on behalf of CONTROLLERS in the UNION. In some cases, CONTROLLERS outside the UNION are also in scope if they market services to customers located in the UNION, for instance websites located outside the UNION, but marketing to EU residents and which process data of EU residents.

It is recommended to clearly inform the Data Subject of what is collected, where it is stored, with whom it is shared, for how long, etc. That is, transparency in praxis, even if Consent is not required for a standard reservation process.

12.2 Commentary to the Flow-Chart

Generally, the information flows from left to right, however the main controller is the hotel and therefore given the letter 'A' as indicator. Multiple Controllers can be in play from right to left, depending on the scenario.

The information in scope here is what is in scope for GDPR, i.e., personal information of various degrees but also behavioural patterns, such as historic stays, future reservations, detailed consumption during a stay including food and beverage, as well as movies watched, telephone numbers dialled, internet addresses visited, etc. that can be linked to a natural person (the Data Subject).

Card holder data, i.e. credit card number (PAN), Expiry Date, Card holder name, etc. is collected during the reservation and stay processes and indicated for general information on the chart. It may be collected at various points in the flow and retained on the reservation record until settlement. Such card holder data is subject to both GDPR and PCI DSS rules (Payment Card Industry Data Security Standards).

12.3 GDPR role(s)

The top row indicates the most likely roles involved, from right to left.

12.3.1 Controller-A (Hotel)

A simple scenario would be a guest staying at a hotel located in the UNION. Walk-in or calling the hotel directly to make a reservation. Check-in, Check-out and settlement happening physically at the Front Desk of that same hotel. In that, the case is clear, the HOTEL is the Data Controller and the data is collected and processed to fulfil a contract with the Data Subject (the person who render the information, consuming the services and pay for the same). Many European hotels still operate like the above. 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 GDPR) and card holder information (subject to PCI DSS).

It is generally accepted that CONSENT is not required in the above situation. A 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 'performance of a contract' (GPDR Article 6.1(b)).

12.3.2 Controller-B (Brand)

Chain hotels are typically branded and therefore identified by the guest as a BRAND unit rather than a locally owned, separate legal entity. This is of course primarily an issue if the reservation is taking place away from the hotel, i.e. via a Branded Web-Site. In that case it can be argued that the BRAND becomes a CONTROLLER – possibly even a JOINT CONTROLLER with 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, namely the HOTEL.

The cooperation between the HOTEL and the BRAND needs to be documented in the form of an agreement between the two controllers (a data sharing agreement), ensuring that they respect each other's role and the GDPR rules on the processing of the data, especially to the handover of data from one CONTROLLER to the other CONTROLLER (normally the brand and the hotel will act as independent controllers sharing data - if they are considered joint controllers they need to jointly agree to the processing of the data).

12.3.3 Processor (CRS)

Based on the debate during the GDPR Workgroup Meeting held on October 19th., 2017, the CRS function was split from the BRAND. 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 and is merely a Processor.

In some situations, the CRS may exist as a legal entity on its own and merely offer white-label call centre and systems functionality to the individual hotels. In other situations, the CRS will be owned by the Brand

and therefore act as an internal service to the 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- Data Processor Agreement between the parties involved. If the Hotel is in the EU while the CRS is outside the EU, data exporting mechanisms should be also identified.

12.3.4 Controller-C (Distributor)

The fourth entity (third Controller) on the top row, is the Distributor, which may be more than one legal entity, i.e. will often by a 'concentrator' like a GDS System (Global Distribution System, like AMADEUS, SABRE, etc.) and a Channel Manager.

Both the GDS and the Channel Manager are often 'transparent' (like 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 are considered a CONTROLLER, parallel to the other CONTROLLERs involved. As mentioned above there might be more Controllers involved for instance a Corporate Travel Function in front of either of these.

When the Travel Agent/OTA acts as a CONTROLLER and strictly collects and processes 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, etc. collects information only for reserving a hotel room, they are likely to have the role of PROCESSORS, while the HOTEL will be 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), they will likely have the role of Data CONTROLLER.

12.3.5 Data Flow

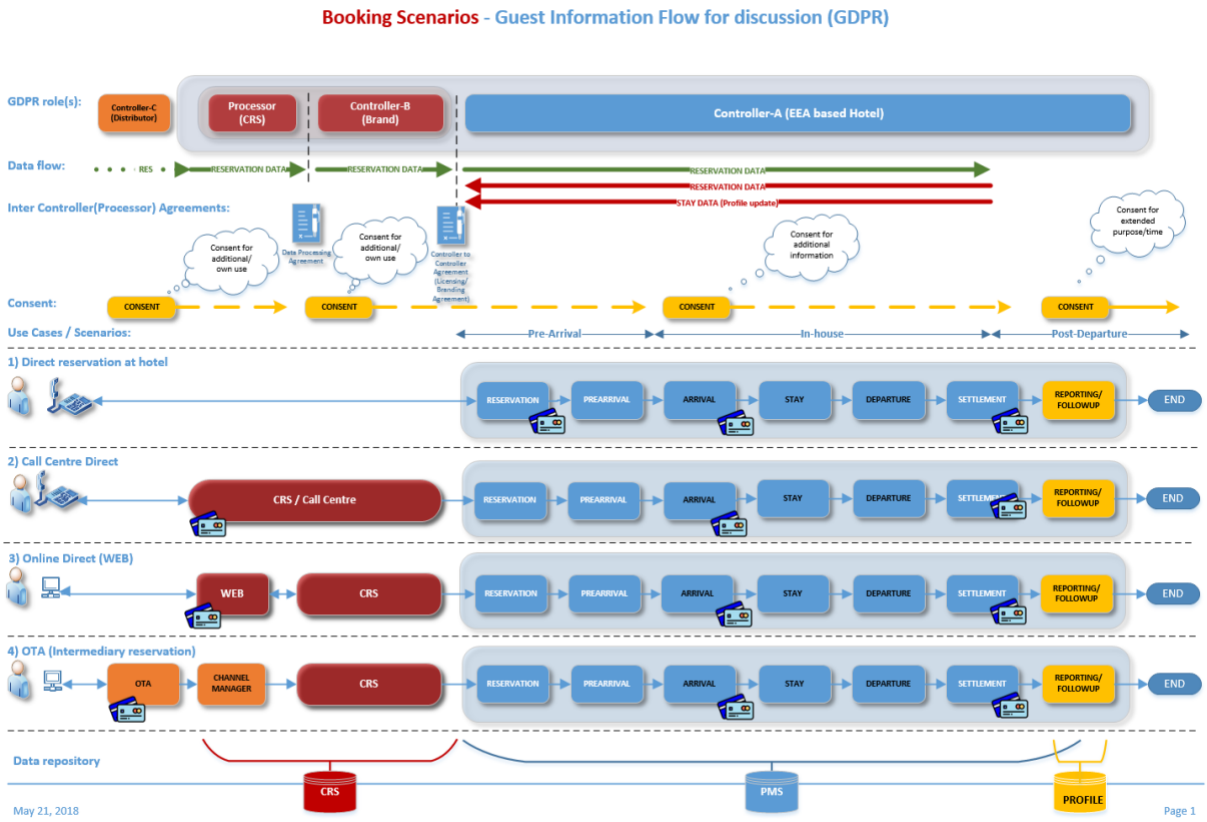

Figure 4 Booking Scenarios

The data flow required to process a reservation is illustrated by a ‘green’ arrow from left to right. The green colour indicating that data can flow without CONSENT and without a Data Export Mechanism (without data transfer restrictions being invoked). This is based on the type of data being limited to what is required to fulfil the contract between the data subject and the HOTEL; and the assumption that the data is flowing into the EU (EEA), not out.

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 locally made reservation 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 centrally (typically branded) guest loyalty program.

It should be noted that there might be numerous less transparent data transfers happening, for instance, as mentioned above, where the Property Management System is offered as a cloud service instead of a local, on-premise system, or where data is extracted to external revenue management systems etc. All such transfers represent ‘red’ arrows and require legal grounds, agreements and information.

12.3.6 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) GDPR. In addition, the transfer of personal data outside the European Economic Area ("EEA") also needs to be supported by the legal grounds that are 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 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); and (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 that seeks to transfer personal data outside the EEA should rely either on:

- 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. 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).

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"): those are 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 terms "companies engaged in a joint economic activity" are understood as covering companies that are under a franchise-agreement (e.g., branded hotels). 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 the EU, the Brand could put in place BCRs.
- Model / Standard Contractual Clauses adopted by the European Commission or by a supervisory authority ("SCCs"); The Commission has so far issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU and one set for the transfer to processors established outside the EU. 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 the EEA.

The best approach should be to:

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

12.3.7 Consent

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’ 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 flow in one direction only, 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. That could be if the OTA or the BRAND wants to make use of the information to support its own interests, such as marketing to the Data Subject, enrolling the Data Subject in a loyalty program, etc.

Equally if the HOTEL collects more data relating to rendering services in-house, that may require Consent or another basis if the services or activities are not covered under the original agreement or contract.

Finally retaining the 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/CRM system.

12.4 Use Cases and Scenarios

12.4.1 Direct booking at the Hotel (or Walk-in)

12.4.1.1 Reservation

The first point of contact can be directly to the hotel, either over the telephone to a local reservation agent or personal at the Front Desk or it can involve one of more prior instances, like a Travel Agency, GDS, CRS/Brand etc. This use case however addresses the direct booking at the hotel.

12.4.1.2 Pre-Arrival

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

12.4.1.3 Arrival

This is the first physical contact with the Data Subject where payment details typically are verified and/or updated, address details collected, maybe passport or other picture ID's details are obtained and recorded.

It is generally understood that 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.

12.4.1.4 Stay

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

If details are collected beyond what is mandated by legislation and/or required as 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.

12.4.1.5 Departure

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

12.4.1.6 Settlement

May happen before the time of departure, at the time of departure or shortly thereafter. Can be in form of a direct bill or most likely payment with a credit card.

12.4.1.7 Reporting/Follow-up

Can include a transfer of information to Brand Loyalty programs or to external loyalty programs of the choice of the Data Subject.

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.

12.4.2 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 as such trigger additional legal considerations.

In case 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 the flow has another legal basis under the GDPR.

If, however the CRS and Call Centre are located outside the EU (EEA) and the data is flowing in both directions i.e. from left to right (from the CRS to the HOTEL) and from right to left (i.e. from HOTEL to the CRS) the HOTEL is effectively exporting information to an entity outside the EU (EEA) which requires one of multiple mechanisms in place to authorize such export of personal data. Please see above under Agreements.

12.4.3 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 the HOTEL is in a lot of ways a duplication of the Call Centre flow above and will trigger the same legal considerations depending on the location of the website and CRS versus the HOTEL.

12.4.4 OTA or other Intermediary (Including Physical Travel Agency Booking via GDS or Web)

The involvement of an intermediary or agent such as an OTA (Online Travel Agency) or a traditional, physical travel agent can possibly complicate matters. If they merely facilitate the minimum data required to process a reservation, i.e. fulfil the contract between the Data Subject and the HOTEL and the data flow from left to right only, they can do so without CONSENT and any kind of Data Transfer Mechanism.

13 Employee Data Flow

The two process flows below are intended to summarize and illustrate two of the biggest 'back-of-house' processes dealing with personal data as identified in GDPR, namely data on employees and other individuals associated with a business unit.

As the retention period and the purposes are very different, the processes have been split in two, namely:

- Pre-employment (recruitment)
- Employment

Be aware that there are numerous other back-of-house processes in scope for GDPR and as such need to be reviewed and documented, for instance:

- e-Mail messaging (including other electronic communication tools such as various chat tools, VOIP, etc.).
- Invoicing and Sales Ledger – where the 'customer' may be a natural person and therefore in scope for GDPR and account contacts who are also natural persons.
- Ordering, Purchase Ledger and related – also here may the supplier by a natural person instead of a company, but also account contacts are in scope for GDPR.
- CCTV or other surveillance tools recording employee movements and activities may be in scope for GDPR.

The following is meant as an explanation of the two mentioned generic processes. Actual process flows need to be obtained from each individual business unit and the charts and text adopted accordingly.

13.1 Recruitment Process

The flow below illustrates all processes involved in the recruitment of new employees. Obviously, there are further internal processes ahead, such as budgetary processes, job-profiling, etc., but as they are not dealing with identifiable personal data, they are not included in these illustrations.

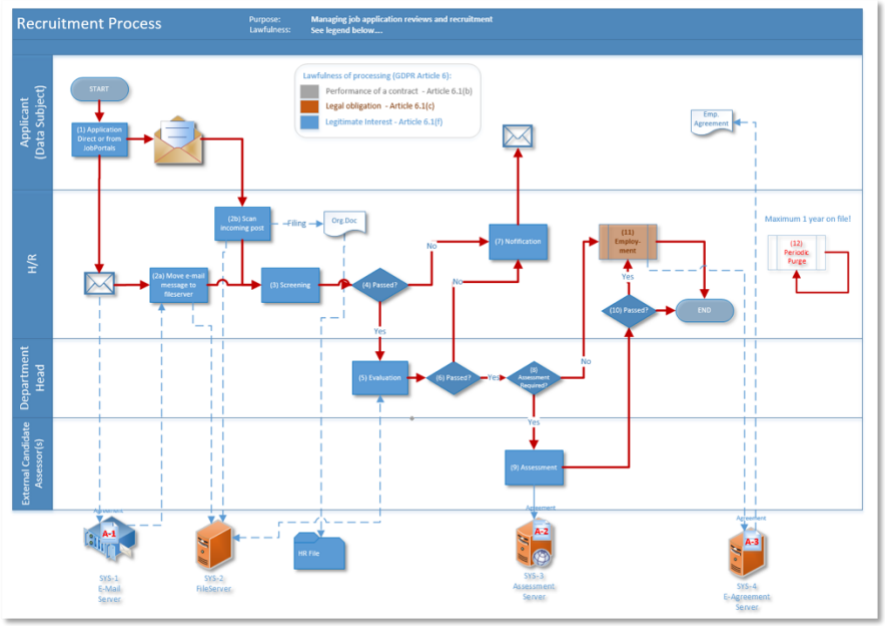

Figure 5 Recruitment Process Flow

Process	(1) Application creation	
Attribute	**Value**	**Comments**
Owner	Applicant (Data Subject)	
Purpose	To apply for a position	May be solicited, i.e. based on a job posting or unsolicited, i.e. a person contacting the business unit to explore options
Lawfulness	Legitimate Interest	The activity is owned by the Data Subject, but the information is received by the business unit who process this in good faith based on Legitimate Interest of the business
LIA required	Yes	
System/Data location	e-Mail system and/or manual files	
Description	The applicant will typically forward a cover letter, a CV and often back-up documentation for education, experience, etc.	

Process	(2a) Receiving application by e-Mail	
Attribute	**Value**	**Comments**
Owner	Human Resources Dept.	
Purpose	Receiving mail	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/ Data location	e-Mail system and departmental file server	If the e-Mail system is an external system or a system supplier has support access, a Data Processing Agreement needs to be in place (marked A-1 below). It is assumed that the departmental file server is local; if that too is an externally hosted server, a DPA is required.
Description	The H/R department will receive incoming e-mail messages, open the message and archive it on	Original message will be deleted from the e-mail system and future review and sharing will be done using internal links to the file server files and folders. Only

	the departmental file server with the appropriate retention period and access restrictions.	authorized individuals with the appropriate access scope will be able to see the documents.

Process	(2b) Receiving letter by post	
Attribute	**Value**	**Comments**
Owner	Human Resources Dept.	
Purpose	Receiving mail	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Manual files and electronic storage on departmental file server as scanned documents	
Description	The H/R department will receive incoming mail, open the envelopes, scan the content and archive the originals in a date-dependent archive set-up where deletion can be done later based on the agreed retention period.	

Process	(3) Screening	
Attribute	**Value**	**Comments**
Owner	Human Resources Dept.	
Purpose	To ‘screen’ applications	Normally carried out by the H/R department
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Manual files and electronic storage on departmental file server as scanned documents	
Description	A kind of ‘sanity check’ against the job requirements, general appearance of the applicant, etc.	

Process	(4) Decision	
Attribute	**Value**	**Comments**
Owner	Human Resources Dept.	
Purpose	Decide if an application/applicant should be presented to the department or a regret message is to be send	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Departmental file server as scanned documents	Only a link will be forwarded to the Department Head in scope; remember, no names in the mail subject or elsewhere
Description		

Process	(5) Evaluation	
Attribute	**Value**	**Comments**
Owner	Line Management – Department Head	
Purpose	Evaluation of the applicant	A link to the original application on the file server will be forwarded to the department head. No circulation of documents by e-mail or manually copied is permitted.
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Departmental file server as scanned documents	Only a link will be forwarded to the Department Head in scope. Remember no names in the mail subject or elsewhere.
Description	Do a deeper evaluation of the applicant and his/her skills versus the job description.	

Process	**(**6) Decision	
Attribute	**Value**	**Comments**

Owner	Line Management – Department Head	
Purpose	Advance the application or reject it	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Departmental file server as scanned documents	
Description		

Process	(7) Notification	
Attribute	**Value**	**Comments**
Owner	Human Resources Dept.	
Purpose	Inform the applicant	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	e-Mail server and original documents on the Departmental file server as scanned documents	
Description		

Process	(8) Further Assessment Decision	
Attribute	**Value**	**Comments**
Owner	Line Management and/or Human Resources Dept.	
Purpose	Decide if the position requires further assessments	Can be a personality test, a back-ground check, reference check, etc.
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	e-Mail server and original documents on the Departmental file server as scanned documents	

Description		

Process	(9) Assessment	
Attribute	**Value**	**Comments**
Owner	Often an external assessor	
Purpose	To do a professional assessment of the applicant	Can be a personality test, a back-ground check, reference check, etc.
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	e-Mail server, original documents on the Departmental file server and an assessment/test server of the assessor	In case of an external assessor being utilized, a DPA (identified with A-2 below) is required
Description	A personality test or just look up	

Process	**(**10) Passed Decision	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	
Purpose	Final decision on employment	Often done in cooperation between the line management and H/R
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	e-Mail server and original documents on the Departmental file server as scanned documents	
Description	Evaluation of the past reviews, tests, etc.	

Process	**(**11) Employment process	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	

Purpose	Formally employs the individual	Employment process – predefined process and outside this flow
Lawfulness	Performance of a contract	
LIA required	No	
System/Data location	e-Mail server and original documents on the Departmental file server as scanned documents	
Description	Initiates an employment contract and trigger the 'on-boarding' process for the new employee	Some businesses use a kind of automatic, electronic contracting software that allows the H/R Department to create and forward an electronic agreement to the data subject for electronic signage. In such cases, a DPA (marked as A-3 below) is required.

Process	(12) Periodic Purge	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	
Purpose	Removes all application records no longer within retention period	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	e-Mail server, original documents as physical records and electronic documents on the Departmental file server	All needs to be removed once the established retention period has been reached. Remember this includes back-up servers, external servers, such as assessment and contracting partners servers.
Description		

13.2 Employment Process

The below is a summary of all process steps or even sub-processes involved during the on-boarding phase, employment phase and finally the termination phase of a person's (data subjects) relation with an employer (business unit).

The below processes take over from the Recruitment Processes outlined above. Please note that this is generic and must be updated in-situ to reflect the actual processes involved at the business unit in question.

Opposite from a number of other processes, this life-time process may actually rely on a number of lawful basis for processing, typically:

- Performance of a contract (GDPR Article 6.1(b)
- Legal Obligation (GDPR Article 6.1(c)
- Legitimate Interest (GDPR Article 6.1(f)

The actual basis is illustrated by a color coding of which the legend is found below.

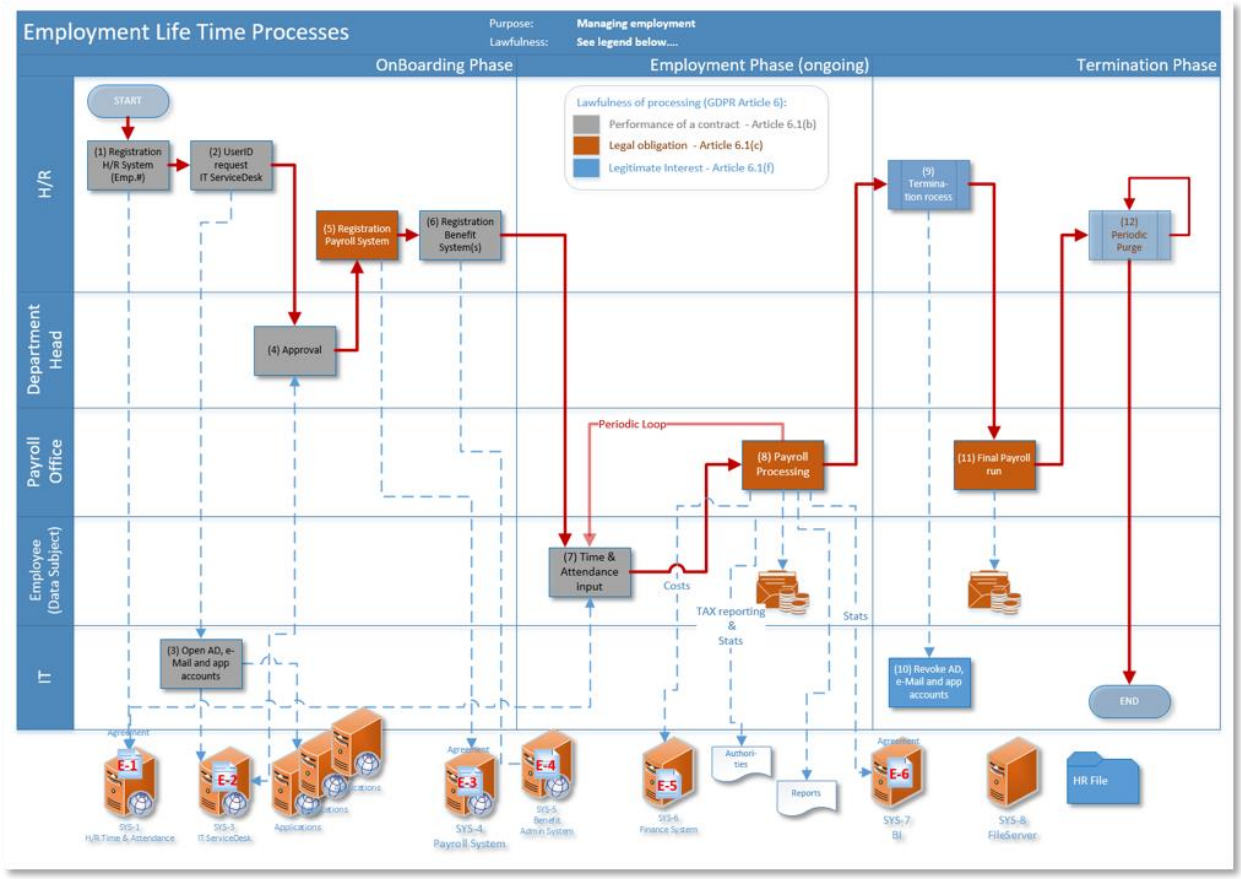

Figure 6 Employment Systems Detail Process

Process	(1) Registration	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	
Purpose	To establish the individual as an employee	This will also normally open a 'file' on the person; can be a manual archive and/or an electronic file system (H/R departmental file server).
Lawfulness	Performance of a contract	
LIA required	No	
System/ Data location	H/R System (SYS-1)	If this system is hosted externally, outsourced as a service, or just has remote access for support by the supplier, a DPA (identified by E-1 below) is required.
Description	Once an individual is approved to be employed, the H/R department will initiate a basic registration in the H/R system which will generate a unique, internal employee number.	The use of governmentally issued ID-numbers, such as a social security number as the internal identifier is no longer permitted. Instead a locally issued number should be used and the social security number or similar can be stored as an attribute on the system and referenced where needed for tax purposes and more.

Process	(2) User-ID request(s)	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	
Purpose	Requesting system access	Ideally, this is a kind of work flow system where by H/R can request system access from IT.
Lawfulness	Performance of a contract	
LIA required	No	
System/Data location	Workflow or Help Desk system	If this system is hosted externally, outsourced as a service of just has remote access for support by the supplier, a DPA (identified by E-2 below) is required
Description	The H/R department will initiate system access (to maintain segregation of duties, it is important	All of this will be done based on the internal employee number

	to split the request of access from those creating the user-id and the access rights).	

Process	(3) Open User Account(s)	
Attribute	**Value**	**Comments**
Owner	IT Department	
Purpose	Creating system user accounts as needed and requested by H/R.	
Lawfulness	Performance of a contract	
LIA required	No	
System/Data location	Workflow or Help Desk system; each individual application including the central authentication system, e-mail system and applications	All system that will process and store personal identifiable data such as user-name, e-mail address, etc. will already for that sake be in scope for GDPR and therefore need a DPA. Those DPAs are not identified herein but are assumed handled elsewhere under each application.
Description	The IT Department creates the user accounts in each system requested based on instructions from H/R and often approval from the Department Head and/or Systems Owner.	All of this will be done based on the internal employee number and logged in the Work Flow/Help Desk System.

Process	**(**4) Approval(s)	
Attribute	**Value**	**Comments**
Owner	Line Management (Department Heads and System	
Purpose	Authorizing access to various applications	
Lawfulness	Performance of a contract	
LIA required	No	
System/Data location	Workflow or Help Desk system	
Description	User Maintenance requests should be automatically routed to the relevant approvers, such as the System Owner and the Department Head of the new employee.	

	All new requests including departmental and role changes need to be approved.	

Process	(5) Payroll System Registration	
Attribute	**Value**	**Comments**
Owner	Human Resources Department and/or Paymaster	
Purpose	Facilitating the agreed compensation and income tax reporting	
Lawfulness	Performance of a contract and/or Legal Obligation	It can be argued which basis to lean on, however in most countries it will be argued with Legal Obligation as the Internal Revenue Services (Tax Authorities) will set specific requirements for the taxation in connection with paying the individual a compensation for performed work.
LIA required	No	
System/Data location	Payroll System (SYS-4)	Normally a hosted or outsourced system and often business process. In either case, a DPA is required, indicated on the flow-chart as E-3.
Description	The employee will be established in the Payroll System with base information, terms, etc. for the system to calculate the gross compensation per pay period, deduct taxes and other agreed deductions.	

Process	(6) Benefit System registration	
Attribute	**Value**	**Comments**
Owner	Human Resources Department and/or Paymaster	
Purpose	Managing specially agreed benefits	
Lawfulness	Performance of a contract	
LIA required	No	

System/Data location	Benefit Management System	Normally a hosted or outsourced system and often business process. In either case, a DPA is required, indicated on the flow-chart as E-4.
Description	Agreed benefits are to be registered and maintained in a structured form.	Only used in certain countries

Process	(7) Time and Attendance registration	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	Partial data entry may be done by the employee (data subject) in that case happening in a dedicated APP. Normally the Department Head will be verifying and approving the data prior to the transfer to the Payroll System.
Purpose	Tracking work schedules, hours worked, absence, etc.	
Lawfulness	Performance of a contract	
LIA required	No	
System/Data location	H/R System or a dedicated Time & Attendance System.	Normally a hosted or outsourced system and often business process. In either case, a DPA is required, indicated on the flow-chart as E-1.
Description	Registration and/or verification of hours worked as well as other variable data for payroll processing, such as mileage, expenses, overtime, etc.	

Process	**(**8) Payroll Processing	
Attribute	**Value**	**Comments**
Owner	Paymaster	
Purpose	Calculating gross and net compensation	
Lawfulness	Performance of a contract and Legal Obligation	It can be argued which basis to lean on, however in most countries it will be argued with Legal Obligation as the Internal Revenue Services (Tax Authorities) will set specific

		requirements for the taxation in connection with paying the individual a compensation for performed work.
LIA required	No	
System/Data location	Payroll System (SYS-4)	Normally a hosted or outsourced system and often business process. In either case, a DPA is required which is indicated on the flow-chart as E-3.
Description	The ongoing processing of base information, variables from time and attendance and external information such as tax rules.	

Process	(9) Termination Process(es)	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	May be initiated from line management/Department Head
Purpose	Winding up an individual's engagement	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Workflow System/Help Desk System	
Description	H/R is responsible for activating the Termination Process, ideally using the Work Flow System that is pre-programmed to inform all relevant functions. Especially, the IT Help Desk needs to be informed and instructed to close all issue user accounts, return of devices handed out, access cards, etc.	

Process	(10) Revoke user accounts	
Attribute	**Value**	**Comments**
Owner	IT Department	As per instructions from H/R

Purpose	Ensure all equipment is returned and systems access revoked	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	Workflow System/Help Desk System and each specific application	
Description	IT needs to make sure all systems and network access is removed including equipment returned and relevant mail messages, files, etc. handed over to the successor.	

Process	(11) Final Payroll Run	
Attribute	**Value**	**Comments**
Owner	Paymaster	
Purpose	Calculating gross and net compensation	
Lawfulness	Performance of a contract and Legal Obligation	It can be argued which basis to lean on, however in most countries it will be argued with Legal Obligation as the Internal Revenue Services (Tax Authorities) will set specific requirements for the taxation in connection with paying the individual a compensation for performed work.
LIA required	No	
System/Data location	Payroll System (SYS-4)	Normally a hosted or outsourced system and often business process. In either case, a DPA is required, indicated on the flow-chart as E-3.
Description	Final processing of base information, variables from Time & Attendance and external information such as tax rules. The final money transfer will only be authorized once all items handed out during the employment are returned and IT has confirmed all user accounts are revoked.	

Process	(12) Periodic purge process	
Attribute	**Value**	**Comments**
Owner	Human Resources Department	
Purpose	Removal of all personal data past retention date.	
Lawfulness	Legitimate Interest	
LIA required	Yes	
System/Data location	All relevant systems and manual files	
Description	Periodic routine – manual and/or automated to remove all data past the retention date (periodically means no less than monthly).	

14 Appendix

14.1 FAQ for Guests, Staff, Ownership

The information in this document and resources is intended to be used by hospitality organizations. However, individuals should validate the requirements and processes identified against their organization's capabilities and contractual arrangements.

To best align the responses to these GDPR FAQs, it is advised to have procedures in place and provide all involved parties easy access to your organization's privacy policy(ies).

What is GDPR?

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 personal data. The Regulation went into effect on May 25, 2018. The GDPR covers both employees and guests.

What is personal data?

Personal data is defined as any data that allows you to identify a living individual. As a result, in the context of hotels, this applies to guests, staff and third parties, such as agency staff, as well as staff at vendors and customers.

The regulation differentiates between personal data such as name, address, telephone number and sensitive personal data which includes biometric, medical, political and religious persuasion, sexuality, etc.

14.1.1 FAQ - Guests

This section is designed to assist guest-facing staff field inquiries from guests.

Staff are encouraged to refer to the organization's procedure handbooks should they encounter questions regarding privacy regulations beyond the commonly asked questions below.

14.1.1.1 What kind and how much of my personal data does your hotel have?

We collect basic information about you when you make a reservation and when you stay with us. Information about you may be passed on to us by other partners involved in your reservation process. We also collect information when you voluntarily complete customer surveys, provide feedback and participate in promotions.

14.1.1.2 Why are you collecting my personal information?

Your personal information is used by us for various purposes, all of which are undertaken in order to provide you with the reliable and timely services you desire. Services include providing your accommodations and allowing you to take full advantage of our hotel's facilities.

14.1.1.3 If my personal data is incorrect, how can it be changed?

There are two options: We can take your information and issue a change request internally. Or you can visit our Privacy Policy on our website and contact us in the location provided on that page. For your record keeping as well as ours, we recommend the second option.

14.1.1.4 How do I request deletion of my personal information?

There are two options: We can take your information and issue a deletion request internally. Or you can visit our Privacy Policy on our website and contact us in the location provided on that page. For your record keeping as well as ours, we recommend the second option.

14.1.1.5 Do you share my personal information with other organizations? If so, who?

We do not disclose or sell your personal information to others for marketing purposes. We use your personal information internally and share it with other people or organizations who need to know it as part of working with us in our normal business activities. We may need to share your personal information with trusted parties that help us provide our services. You can review our Privacy Policy for more details.

14.1.1.6 How long will your hotel and your partner organizations hold my personal information?

Historic stay details are stored to allow us to recognize you on possible future visits to the hotel and ensure a consistent service delivery to suit your preferences. There are law-enforcement and financial regulations that dictate that certain data is retained for long periods of time.

14.1.2 FAQ - Staff

This section may include contractors, suppliers, and others that do business on behalf of the hotel. This may also include potential employees or candidates. Please note that privacy policies for employees may differ from customers.

Staff are encouraged to refer to the organization's procedure handbooks should they encounter questions regarding privacy regulations beyond the commonly asked questions below.

14.1.2.1 Why is personal information collected about me?

Data is collected to manage your employment agreement or evaluate your employment application. This enables us to meet payroll, insurance, taxation, permits and other legal requirements as well as operational needs.

14.1.2.2 What personal information is being collected about me?

Your personal information is used by us for various purposes, all of which are undertaken to manage your involvement with the organization. Our purposes range from the hiring process through to the scheduling and compensation. Information includes basic information such as name and address, etc. Other information may be included in our operational systems, such as:

- Human Resources
- Work Scheduling
- Payroll
- Access Control

14.1.2.3 Do you share my personal information with other organizations? If so, who?

We utilize business partners to process your personal information on our behalf. Those partners only process your personal information at our direction. The usage of your personal information will be done only in accordance with your consent, except in cases where required by law.

If you used a recruiter or other service in an effort to gain employment, please contact that service or provider for how they use your information. That service may have policies that differ from your current employer.

14.1.2.4 How long will the organization and related entities hold my personal information?

We will retain your data as long as we are legally required to do so, and for as long as we have a relationship with you. We may also have retention policies that cover employment records.

14.1.2.5 How do I request a copy, alteration or deletion of my personal information?

Please contact the human resources or personnel department for more information. Please note that for legal reasons, we may not be able to delete or alter your data in some circumstances.

14.1.3 FAQ - Data Controller/Party with Fiduciary Responsibility

This section is intended to aid business persons with data controller responsibilities in relation to GDPR. Data Controllers are encouraged to seek professional assistance (i.e. legal) for validation.

14.1.3.1 Do I have to worry about GDPR?

Yes, you need to conduct a thorough evaluation of your business processes and customers to understand if you are subject to the GDPR. Here are some key insights to help you identify your risks:

- Is your company based in the EU?
- Are you part of an organization that has a controlling presence in the EU?
- Do you do direct marketing to people located in the EU?
- Do you use any processors that are centered in the EU?

If you answered YES to any of the above questions, you may be subject to GDPR.

Further, if you are subject to GDPR, and export or transfer data out of the EU, you must have legal mechanisms (privacy shield, binding corporate clauses, etc.) in place that provide protections to that data.

14.1.3.2 If I am subject to GDPR, what do I do?

The following steps are recommended:

- Identify and document business activities that result in data processing, collection and retention
- Find out what data you collect about your employees and customers
- Find out which systems are involved in data processing
- Find out who has access to data
- Identify the purpose of why you process data
- Identify the legal basis to process data
- Stop unlawful processing of data
- Ensure you have data processing agreements in place for vendors or third parties involved in data processing, including cross-border data transfers
- Publish privacy policies that reflect GDPR requirements
- Identify and document a Standard Operating Procedure that identifies how the company responds to Personal Data Requests (requests for data, changes, deletion)
- Identify and document a Standard Operating Procedure that identifies the appropriate steps in the event of a data breach
- Communicate GDPR requirements internally
- Conduct awareness training
- Decide if you need a formal Data Protection Officer (DPO) position

14.1.3.3 Where does my responsibility end and my brand's begin?

It's important to understand your business processes to help identify where your responsibilities lay. Individual hotel operations are generally the owner's accountability, but this is further complicated by a management company's involvement.

14.1.3.4 Where does my responsibility end and my management company's begin?

If management of the property is contracted to an external party (in full or part), the contract should specify how the 3rd party should handle personal information of guests and/or staff. If you have not updated your management agreements since (or prior to) the enforcement date of GDPR, you should evaluate your exposure and update those agreements accordingly. These contracts should clearly identify whom the controller is.

It helps to identify which entity (owner, management company, other) has fiduciary responsibilities for the property. The responsible party is accountable for GDPR compliance but may enforce contractual responsibilities for compliance to GDPR upon a third party, such as a management company.

It is also important to identify the legal entity (as opposed to the trading entity) that is a controller of personal information in the privacy policy.

14.1.3.5 Where does my responsibility end and my solution providers' begin?

Your solution providers are responsible for executing your instructions - you are always responsible for the data within the systems you procure. In other words, you are accountable for what your processors (solution providers) do, and they are responsible for executing your instructions.

In the context of GDPR, your solution providers are likely processors that use personal information at your direction. As a result, you need clear instructions and privacy related policies within your processing agreements that dictate how that data should be used, processed, and exported. In addition, it should be clear that those agreements cascade to third parties that the processor sub-contracts. These instructions should reflect your business processes.

It is also important to note that Controllers are accountable for personal information issues (breaches, GDPR violations) regardless of whether they occurred via the controller or the processor. Because of this, it is important to have a plan and clearly defined obligations in place if a violation or security issue occurs.

14.2 Enforcement Actions

The following enforcement actions are examples and are current as of the publication of this document. Other enforcement actions are likely to occur and are easily searchable on the internet.

On May 25, 2018, Facebook and Google were hit with a raft of lawsuits accusing the companies of coercing users into sharing personal data. The lawsuits, which seek to fine Facebook 3.9 billion and Google 3.7 billion euro (roughly $8.8 billion in dollars), were filed by Austrian privacy activist Max Schrems, a longtime critic of the companies' data collection practices.

The French activist group, La Quadrature du Net, filed complaints with CNIL (the French data protection authority) against Google, Apple, Facebook, Amazon, and Microsoft, on behalf 12,000 individuals. This case is also based on the claim that internet platforms used a 'forced consent' mechanism.

None of Your Business (NOYB) filed complaints against Facebook in Belgium, Germany and Austria; and against Google in France over 'forced consent.' NOYB argued that data protection authorities should impose prohibitive fines to protect the privacy of Facebook, Instagram, WhatsApp, and Android users. The maximum possible fine in this case amounts to 7 billion Euro.

France's DPA announced formal notice proceedings against Fidzup and Teemo — two mobile ad tech companies — for failing to obtain GDPR-compliant consent from individuals when processing their

geolocation data for advertising purposes. (Teemo was also put on notice for retaining geolocation data for 13 months, which France's DPA said was too long to justify the purpose of targeted advertising.)

In September, Dr. Johnny Ryan, chief policy and industry relations officer of Brave, a web browser that blocks ads and website trackers, filed a complaint with several DPAs, asking them to investigate certain ad tech companies for "data breaches" caused by behavioral advertising. According to the press release, "every time a person visits a website and is shown a 'behavioral' ad on a website, intimate personal data that describes each visitor … is broadcast to tens or hundreds of companies … in order to solicit potential advertisers' bids for the attention of the specific individual visiting the website. Dr. Ryan alleges that a data breach occurs because this broadcast, known as a 'bid request' in the online industry, fails to protect these intimate data against unauthorized access."

At the end of October, France's DPA issued a notice to Vectaury, another mobile ad tech company, for its failure to obtain GDPR-compliant consent for its data processing activities. Vectaury collected data both through its SDK and through real-time bidding offers initially transmitted via auctions for advertising inventory. Vectaury retained the data it received through the bidding offers for use beyond responding to the bid. Although Vectaury implemented a consent management platform as part of the TCF, France's DPA found that the consent language failed to notify the users how their data would be used and who it would be shared with.

On November 27, 2018, seven consumer groups who were members of BEUC filed complaints against Google with their national data protection authorities. These complaints are based on new research published by the Norwegian consumer council, Forbrukerrådet, which look at how Google continuously tracks the location of its users through a number of different technologies.

In the United Kingdom, British Airways faces a class-action lawsuit for a breach of the credit card payment details concerning approximately 380,000 plane tickets.

Prompted by a consumer complaint, the Irish Data Protection Commissioner recently initiated an investigation into t.co, Twitter's link-shortening system. Twitter allegedly declined to provide t.co data in response to the consumer's access request, arguing that to do so would require disproportionate effort.

14.3 Supervisory Authorities

The European Data Protection Board (EDPB) has not issued its annual report; however, some websites have started collecting statistical information they obtain through open record requests.

The EDPB claims that thousands of complaints have been lodged across Europe. This number is likely even higher when we take into consideration that the GDPR also allows citizens to file lawsuits directly with courts. Current complaint numbers can be found on https://www.iapp.org.

Nearly 13,000 separate data breach notifications have been sent by businesses and other organizations since the GDPR was implemented. Many data protection authorities have indicated a sharp increase in the number of data breach notifications when compared to the same period last year. According to information provided to a third party website by the UK ICO, the highest number of data breach notifications concerned the disclosure of data (nearly 4,000 cases). We do not have any information about the categories of breaches from other countries.

According to Microsoft, as of September 2018, over five million people from 200 countries have used Microsoft's new privacy tools to manage their data, and over two million of those requests came from the U.S.

14.3.1 European Data Protection Board

The EDPB has not issued any binding decisions.

On November 26, 2018, the EDPB published Guidelines 3/2018 on the territorial scope of the GDPR (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf).The proposed Guidelines are open for public consultation until January 18, 2019. The Guidelines provide some clarification around the boundaries of what constitutes an establishment in the EU, the status of tourists and factors that determine whether data subjects in the EU are being targeted. The EDPB also provides some guidance on the conditions of appointment of an EU representative for non-EU controllers and processors.

The Guidelines clarify that the GDPR apples if one of these two criterions is met: (1) the "establishment" criterion, as per Article 3(1); or (2) the "targeting" criterion as per Article 3(2).

1. Application of the Establishment Criterion (Article 3(1))

The Guidelines state that a controller or processor will be considered to have an establishment in the EU if it exercises a real and effective activity (even a minimal one) exercised through stable arrangements, regardless of its legal form (e.g., subsidiary, branch, office, etc.), in the territory of a Member State. The threshold for "stable arrangement" can be quite low (e.g., presence of a single employee or agent of the non-EU entity in the EU, provided that such employee or agent acts with a sufficient degree of stability).

However, the non-EU entity may not be considered as having an establishment in the EU merely because, for example:

- Its website is accessible from the EU;
- It has designated a representative in accordance with Article 27 of GDPR; or
- It uses a data processor established in the EU.

The Guidelines contain an important and relevant example:

Example: A hotel and resort chain in South Africa offers package deals through its website, available in English, German, French and Spanish. The company does not have any office, representation or stable arrangement in the EU. In this case, in the absence of any representation or stable arrangement of the hotel and resort chain within the territory of the Union, it appears that no entity linked to this data controller in South Africa can qualify as an establishment in the EU within the meaning of the GDPR. Therefore, the processing at stake cannot be subject to the provisions of the GDPR, as per Article 3(1). However, it must be analyzed whether the processing carried out by this data controller established outside the EU can be subject to the GDPR, as per Article 3(2).

2. Application of the Targeting Criterion (Article 3(b))

The EDPB clarified that the processing of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR as long as the foreign controllers or processors do not specifically "target" or "track" individuals in the EU pursuant to Article 3(2) (a) or (b).

Some attorneys have concluded that these guidelines clarify that U.S. hotels that are available to EU guests, but do not specifically target or track them, do not fall under the GDPR. I will need to research this issue more carefully and recommend that we monitor this guideline. The consultation period for public opinion ends on January 18th.

On December 4, 2018, the EDPB published Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR along with Annex 1 which provides guidance for the specification of "additional" accreditation requirements with respect to ISO/IEC 17065/2012 and in accordance with Articles 43(1)(b) and 43(3) of the GDPR.

The document sets out suggested requirements that a supervisory authority shall draft and apply during the accreditation of a certification body for a certification mechanism with supervisory authority or EDPB approved criteria. While the annex should be read in conjunction with ISO/IEC 17065/2012, GDPR has precedence.

14.3.1.1 Opinions

Article 35(4) of the GDPR states that the supervising authorities of the EU Member States must establish, publish and communicate to the EDPB a list of processing operations that trigger the DPIA requirement under the GDPR. The vast majority of EU member states have submitted their lists. The only member states that have not complied with this requirement are Cyprus and Spain.

The EDPB has published opinions on the draft lists submitted. In some cases, the EDPB requests that the supervising authorities include processing activities in their list or specify additional criteria that, when combined, would satisfy the DPIA requirement. In other cases, the EDPB requests that the supervising authorities remove some processing activities or criteria not considered to present a high risk to individuals. The purpose of the EDPB opinions is to ensure the consistent application of the GDPR's DPIA requirement and to limit inconsistencies among EU Member States with respect to this requirement. Importantly, however, the national lists will not be identical because, in establishing DPIA lists, the supervising authorities must take into account their national or regional context and national legislation.

The EDPB has emphasized that the national DPIA lists are aimed to improve transparency for data controllers, but they are not exhaustive.

14.3.2 Country Level Enforcement

Three enforcement actions have been initiated alleging violations of the GDPR. The total fines issued for GDPR violations total EUR $424,800. Details of the enforcement actions are below.

14.3.2.1 Germany

Personal data of approximately 330,000 users of a chat platform were compromised and then made publicly available by hackers in September 2018. As part of the data breach notification, the provider disclosed that the users' passwords were stored in an unencrypted form. The DPA of the German state of Baden-Württemberg considered this a violation of the obligation to implement adequate security measures (Article 32 GDPR) and imposed a fine of EUR 20,000.

When deciding on the amount of the fine to be imposed, the DPA considered the overall financial impact of the security breach (including the fine) on the provider and also considered in particular that the platform provider:

- Notified the breach to the DPA and to the data subjects in due time
- Was fully transparent and cooperated fully with the DPA
- Implemented both the legal requirements and the recommendations of the DPA and promptly increased the protection levels for personal data

14.3.2.2 Austria

An entrepreneur in Austria had installed a CCTV camera in front of his establishment, also recording a substantial section of the sidewalk. The Austrian DPA considered this a violation of the GDPR because it does not recognize any legitimate interests of companies (or entrepreneurs) to put public spaces under CCTV surveillance. Moreover, the video surveillance was not sufficiently marked, violating the transparency obligation under the GDPR. Taking into account the annual income of the entrepreneur, the Austrian DPA imposed a fine of EUR 4,800 for illegal video surveillance activities.

14.3.2.3 Portugal

After carrying out an inspection at a Portuguese hospital, the Portuguese DPA found that the hospital's account management practices were deficient because:

- There were 985 active accounts for doctors even though only 296 doctors worked at the hospital
- Any doctor had access to all patient files, regardless of the doctor' s specialty.

The hospital argued that it was not responsible for these deficiencies because it used the IT system provided to public hospitals by the Portuguese Health Ministry. However, the Portuguese DPA rejected this argument and found that it was the hospital's responsibility to ensure that adequate security measures were implemented. For violating this obligation, the Portuguese DPA imposed a fine of EUR 400,000 on the hospital.

14.3.2.4 UK ICO

The UK ICO has published a Guide to Data Protection, which is for data protection officers and others who have day-to-day responsibility for data protection. It covers the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK. It is unclear when this guide was published or whether it has been updated since the GDPR came into effect.

ICO states that its official guidance will be updated soon to reflect changes since the Data Protection Act 2018 became law.

14.3.2.4.1 Enforcement Actions

The UK ICO has not issued any GDPR-related fines. On July 6, 2018, the UK ICO issued an enforcement notice to AggregateIQ Data Services Ltd. (AIQ), a Canadian-based company. AIQ processed personal data on behalf of UK political organizations, in particular Vote Leave, BeLeave, Veterans for Britain and the DUP Vote to Leave. The ICO found that AIQ failed to comply with Articles 5 (1)(a)-(c), 6, and 14 of the GDDPR. This is because AIQ processed personal data in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing. As a result, AIQ was ordered to cease processing any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes.

Since May 28, 2018, the UK ICO has initiated 17 enforcement actions; however, they all alleged violations of either Directive 95/46/EC or the Privacy and Electronic Communications Regulation. The total fines issued during this period total £3,077,000.

Date	Data Controller	Description	DPA/PECR	Fine Amount
6/11/18	Gloucestershire Police	Gloucestershire Police fined for revealing identities of abuse victims in bulk email	DPA	£80,000

6/18/18	British Telecommunications Ltd	British Telecommunications plc (BT) has been fined £77,000 by the Information Commissioner's Office after it sent nearly five million nuisance emails to customers	PECR	£77,000
6/18/18	Our Vault Ltd	Our Vault was fined £70,000 for making 55,534 unsolicited marketing calls to people who had registered with the Telephone Preference Service (TPS) and had not consented to being contacted by the company	PECR	£70,000
7/5/18	Independent Inquiry into Child Sexual Abuse	Independent Inquiry into Child Sexual Abuse (IICSA) fined £200,000 for revealing identities of abuse victims in mass email	DPA	£200,000
7/27/18	AMS Marketing Limited	AMS Marketing Ltd, of Peacehaven, made the calls to people who had opted out of receiving marketing calls by registering with the Telephone Preference Service (TPS)	PECR	£100,000
8/8/18	Lifestyle Marketing (Mother and Baby) Ltd	Emma's Diary fined £140,000 for selling over a million records for political campaigning	PECR	£140,000
9/3/18	Everything DM Ltd	Marketing agency fined £60,000 for nuisance emails	PECR	£60,000
9/19/18	Equifax Limited	Credit reference agency Equifax fined for security breach	DPA	£500,000
9/26/18	Bupa Insurance Services Limited	Health insurance company fined £175,000	DPA	£175,000
Date	Data Controller	Description	DPA/PECR	Fine Amount
10/3/18	Heathrow Airport Limited	Airport fined £120,000 following loss of unencrypted USB stick	DPA	£120,000
10/24/18	Facebook Ireland Ltd / Facebook Inc	Data Controller(s) fined for serious breaches of the	DPA	£500,000

		first and seventh data protection principles in respect of the processing of the personal data of 'UK Users'		
10/31/18	ACT Response Limited	Company fined £140,000 for making marketing calls to TPS subscribers	PECR	£140,000
10/31/18	Secure Home Systems	Company fined £80,000 for making calls to numbers registered with the TPS	PECR	£80,000
11/23/18	Solartech North East Ltd	Company fined £90,000 for making calls to numbers registered with the TPS	PECR	£90,000
11/23/18	DM Design Bedrooms Ltd	Company fined £160,000 for making nuisance calls to TPS subscribers	PECR	£160,000
11/26/18	Uber	Uber fined for failing to protect customers' personal information during a cyberattack	DPA	£385,000
12/10/18	Tax Returned Limited	Company sent unsolicited text messages for direct marketing purposes without the consent of the recipients	PECR	£200,000

[1] https://www.eugdpr.org
[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.
[4] Article 40
[5] Articles 33 & 34
[6] See especially Article 30 paragraphs 1, 3, 4, 5
[7] See Article 26: Joint Controllers

15 Technical and Organizational Measures

This section provides an indication of the sort of measures to adopt and is not intended to be exhaustive.

15.1 Organizational Checklist

- Ownership of the GDPR program including clear Board sponsorship
- Establish a Data Protection/Management office; possibly appoint a Data Protection Officer
- Mapping data flows and assigning roles to users and what data that they can view, create, amend or delete
- GDPR training to educate staff in how to handle personal data
- Clear processes:
    - Securing consent to market/communicate/process data
    - Securing consent to process a child's data from the parent/guardian
    - Responding to requests for documents/information that include personal data, e.g. guest folio. Is the person really the data subject? Is the requester entitled to receive it?
    - Handling requests from data subjects
    - Breach management
- A Data Retention Policy including the processes to effectively implement it
- Data Processing Agreements with Data Processors
- Data Sharing Agreements with Controllers to which data is passed or from which data is received
- Legal instruments for the cross-border transfer of data outside of the EU to countries which are not in the EEA or for which there is no adequacy decision. E.g. EU-US Privacy Shield or Standard Contract Clauses
- Access control to back-of-house areas
- Access control to IT comms rooms and cabinets

15.2 Technical Checklist

- Separate administration and user accounts for IT staff
- Secure infrastructure design including networks, servers, storage, clients and connectivity to third parties
- Secure operations including the monitoring, management and regular review of all systems and infrastructure
- Systems access control including unique, named and unshared user accounts and passwords.
- Security solutions such as anti-virus/malware protection/end-point protection/firewalls/intrusion detection.