GDPR
FOR HOSPITALITY

schellman
Quality, above all.

During our interactions with organizations preparing for the GDPR, we have come across some frequently asked questions, some of which pertain to the hospitality industry. We have collected those questions and have put them together here in this FAQ document.

For more answers to your GDPR questions, you can skip to the last page to contact our team directly.

How does the GDPR affect the hospitality industry?

The GDPR is an industry agnostic requirement that could apply to any business under certain conditions. As detailed in Article 3, the text provides an explanation on the circumstances that could expose an organization to the new law. Specifically:

1. If an organization has establishment in an EU member state
   Example: a hotel chain has a physical location in Paris, France

2. If an organization offers goods and services to EU citizens (irrespective if a physical location is in the EU)
   Example: targeting EU citizens to purchase services

3. If an organization monitors the behavior of EU citizens within the EU (irrespective if a physical location is in the EU)
   Example: tracking individuals online to create profiles of users to predict preferences or behaviors

Like any industry, organizations in the hospitality industry should perform an assessment to determine whether they fall into scope of the Regulation. Where in doubt, seek the advice of legal and privacy experts.

Is it important to evaluate our data collection practices (data inflows)?

Data collection activities often evolve over the course of an organization's lifetime. In practice, even a small change to a website booking form, newsletter registration, restaurant reservation, or property management system may have major implications on new data inflows or data sharing channels with external entities. Because of the changing nature in data collection and usage, organizations should allocate resources to conduct a thorough data inventory and data flow mapping exercise to, at a minimum, evaluate and document:

1. Types and categories of data fields collected
2. Purposes for collecting personal data
3. The points of data collection (e.g. registration forms, travel agents, booking system)
4. The geographic location of the organizations infrastructure (servers and databases) and interconnected systems and repositories
5. Who has access to the personal data records and how access is controlled

Once the structure of the data flows are confirmed, the organization should be prepared to evaluate any planned changes that may impact data collection activities through an assessment (e.g. data protection impact assessment) to ensure that they comply with the principles of the GDPR.

In addition, this process will also support the preparation of the organization's record of processing activities requirements (Article 30) and in clarifying where data subject requests may apply and what internal systems are impacted (Articles 15-22).

What personal data elements are important to consider in meeting GDPR?

Organizations in the hospitality industry may collect, process, and store a variety of personal data on their guests and employees. This data may include a combination of personal and sensitive information (i.e. special categories) and could require specific handling requirements and technical safeguards to protect it.

According to the GDPR, "personal data" can be classified as any information relating to an identified or identifiable natural person. In particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

Hotels can have several important personal data elements that need consideration, including:

- **Guest Data:** name, gender, home address, work address, telephone number, e-mail address, data of birth, passport details
- **Stay Details:** dates of stay, purchases, guest, children age
- **Financial details:** credit card and payment information

What personal data elements are important to consider in meeting GDPR?

In addition, the Regulation differentiates sensitive data categorized as "special categories" which require specific attention of the organization. These "special categories" include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Areas to consider for "special categories" of data:

- **Employment data:** application or employment information that specifies racial or ethnic origin, trade union membership, or criminal history
- **Health-related data:** disability information for room preferences, food restrictions

To any extent, organizations must collect, store, or process some level of personal data; in understanding the types of data they collect or process, the organization will be in a better position to develop a plan handle that data based on legal requirements.

Is it important to assess data sharing arrangements with third-parties (data outflows)?

Data sharing activities can take place with a variety of intra-company and external entities, whether it be service providers or business partners. Regardless of the circumstances, these practices will need to be formally evaluated to ensure that data sharing is controlled and protected by a type of data processing agreement, where applicable. In addition, the evaluation may address the following considerations for each data sharing arrangement:

1. Purposes for sharing personal information with another organization
2. Personal data elements that are shared (is it minimized to what is necessary)
3. Option to anonymize personal data fields prior to the transfer
4. How is the information transferred and is it appropriately protected?
5. Will information be shared or transferred outside of the EEA?
6. Can the third party facilitate data subject access rights (Articles 15-22) where requested by the organization (i.e. right to be forgotten)?

Is it important to assess data sharing arrangements with third-parties (data outflows)?

It is also important to understand the roles of the entities that share personal data. These entities are classified by the GDPR as:

1. Controller: determines the purposes and means of the processing of personal data.
   Example: Hotel collecting and processing personal data collected from its guests

2. Joint Controller: where two or more controllers jointly determine the purposes, and means of processing.
   Example: Corporate offices and subsidiary/franchisee mutually processing personal data of its guests

3. Processor: processes personal data on behalf of the controller.
   Example: travel agents, hotel booking portals, direct marketing systems, CCTV and security services, third party online chat systems processing personal data as part of a contract with a hotel

As part of this review, organizations may also need to assess the requirement for obtaining valid consent from the data subject prior to a transfer; and ensure that the data sharing arrangements are legal, transparent, and communicated through a privacy notice or customer agreement.

When and how should the organization inform data subjects of privacy practices?

Transparency is a key principle of the Regulation and obligates an organization to unambiguously describe, in writing, the details of its processing activities and privacy practices via a notice, customer agreement, consent form, or a similar company-specific documentation. Each industry may have its own unique format for communicating business and processing activities to their customers. Therefore, organizations in the hospitality industry should recognize the expectations of their customers and the requirements of applicable law while drafting a privacy notice to avoid confusion which could lead to a customer complaint to a data protection authority.

These notices may be directed towards multiple audiences; for example, to describe:

1. **Guests and Customers:** the use of customer personal data collected for reservations, marketing, membership, and analytics purposes
2. **Online Visitors:** the use of cookie information collected while using the website
3. **Employees:** the use of a data subject's personal data to process applications, conduct background screenings, or to evaluate candidate's qualifications via inquiries

As per the Regulation, organizations are required to provide these notices at the time when personal data are obtained. As there may be several data collection points for organizations in the hospitality industry, possible areas to consider could include:

- Online reservations systems with suitable privacy notices
- Trained employees competent in conveying privacy details for information collected via phone call; in particular, where calls are recorded

Organizations should refer to Articles 13-14 for specific information elements that must be addressed in the privacy notice; and, leverage recommendations from location data protection authorities regarding local codes of practice.

Should I be familiar with data subject rights?

Under the GDPR, organizations could be required to offer certain privileges to their customers regarding the processing and storage of their personal data. Where an organization has determined that it is applicable to the Regulation and serves in the role of a "Controller", they should be educated in the following rights:

1. **Right to be informed**
   Example: A customer is entitled to information about your processing activities, usually provided via a privacy notice.

2. **Right of access by the data subject**
   Example: If requested, can you provide information about the use of a customer's personal data and what data elements you store about them?

3. **Right to rectification**
   Example: If requested, can you provide a customer with the ability to correct or update their personal data stored on your systems?

4. **Right to erasure**
   Example: If requested, can you completely erase a customer's personal data from your systems (including interconnected systems/repositories)?

5. **Right to restriction of processing**
   Example: If requested, can you suspend processing personal data of a customer where they contest the use of their information?

6. **Right to data portability**
   Example: If requested, could you transmit a customer's personal data to another hotel group?

7. Right to object
   Example: If requested, could you cease processing of a customer's data where they object to the processing for direct marketing purposes (e.g. promotional e-mail campaigns)?

8. Right to not be subject to automated processing
   Example: If requested, could you cease processing a customer's personal data where they object to automated decision-making activities (where applicable)?

Organizations should begin preparing for how they will handle such requests from their customers. Importantly, mismanagement of these requests may lead to a complaint which could prompt an investigation by a supervisory authority. In practice, appropriately designed policies and procedures for handling access requests could prepare the organization in handling the request in a timely manner.

What do my breach notification procedures need to include to avoid fines?

Breach notification requirements differ between controllers and processors. It is important that your organization has determined its role in personal data collection and processing under the GDPR before addressing breach notification procedures. The organization should also ensure that their role and the roles of their customers and vendors are established in contracts (legally) to ensure that all parties are aware of their part to play in the breach notification process.

The GDPR places responsibility for breach notification to supervisory authorities and data subjects on controllers as they have ultimate responsibility for the safeguarding of personal data. Controllers are required to notify supervisory authorities within 72 hours of a breach and data subjects without undue delay. It is important to note that supervisory authorities are only required to be notified of a personal data breach if a risk to the rights and freedoms of natural persons is present and data subjects are only required to be notified of a personal data breach when the breach is likely to result in *high* risk to the rights and freedoms of natural persons. The notification to supervisory authorities and data subjects, when applicable, should include the information specified under Article 33, such as:

1. Nature of the breach, categories of and approximate number of data subjects, and categories of and approximate number of personal data records (supervisory authority only)
2. Name and contact details of DPO or other contact
3. Likely consequences of the personal data breach
4. Measures taken or proposed to address the breach and mitigating measures for possible adverse effects

What do my breach notification procedures need to include to avoid fines?

The controller is also responsible for keeping a record of all breaches, facts relating to the breach, as well as the effects and mitigating measures put in place to address the breach and prevent future breaches. Controllers should also familiarize themselves with Article 34, as there are certain derogations for providing breach notification to data subjects.

As the controller is responsible for all the above, the main responsibility of processors is to notify the controller without undue delay of all relevant information when it becomes aware of a personal data breach. Processors are also responsible for aiding in the mitigation of identified breaches, especially if the breach occurred at the processor level.

Do I need to improve anything from a security perspective to meet GDPR requirements?

In short, yes. Odds are that the organization has approached organizational policies, procedures and controls from a security standpoint using a traditional risk assessment (for example, asset based risk assessment under SOC 2 or ISO/IEC 27001). The requirements of the GDPR specify that "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" of "varying likelihood and severity for the rights and freedoms of natural persons" be implemented.

If the organization's current risk assessment and practices can evidence that risks to the rights and freedoms of natural persons have been considered, no further steps may be required. However, in the instance that the organization's current risk assessment and practices do not factor in the risks to natural persons by analyzing risks at the personal data level and the processing and transfers involved therein, the organization may need to reassess implemented security controls to ensure those risks are covered.

In addition to factoring in the risks to natural persons, the GDPR specifies that the security of processing should also include the following, *as appropriate*:

1. The pseudonymisation and encryption of personal data
2. Confidentiality, integrity and resilience of personal data
3. Availability and access of personal data in the event of a physical or technical incident
4. Regular testing, assessing and evaluation for the effectiveness of technical and organization measures

What is this I keep hearing about the "right to be forgotten"?

The right to be forgotten is the same premise as the right to erasure. The right to erasure is one of the many rights of the data subject established by the GDPR and requires organizations to erase all personal data regarding the data subject without undue delay when one of the following scenarios is present:

1. The personal data is no longer necessary to fulfill the purpose(s) for which the data was collected or processed
2. The data subject withdraws consent (where only consent was used as the lawful basis for processing)
3. The data subject objects to processing
4. The personal data was unlawfully collected/processed
5. A legal obligation exists where the controller must comply in accordance with Union or Member State law
6. The personal data was used to provide information society services

It is important for organizations to be familiar with the related articles as there are some derogations for specific situations specified in the GDPR.

How does the GDPR apply to marketing practices?

Marketing practices are specifically addressed in several areas of the GDPR, the main ones being direct marketing and profiling. Article 21 requires that data subjects be provided the option to opt-out of processing for direct marketing purposes, which includes profiling to the extent that it is related to direct marketing. When the data subject opts out of said processing, personal data can no longer be utilized for direct marketing purposes.

In addition to providing opt-out rights to data subjects, the GDPR specifically requires that data subjects be notified of their right to opt-out "at the latest at the time of the first communication with the data subject". The stereotypical example here would be including links for the privacy policy/notice and opt-out/unsubscribe at the bottom of the initial email.

What kind of privacy awareness training should we be providing to employees?

Privacy awareness training should be considered as pertinent as security awareness training for impacted employees with GDPR setting hefty penalties for privacy practices not being followed or the data subjects' personal data being collected or processed unlawfully. It is important to educate the impacted employees of the workforce on the organization's privacy policies and practices as well as the applicable laws.

It may be in the organization's best interest to provide a general privacy awareness training to all employees with more detailed privacy awareness training to those in departments with personnel that interact directly with data subjects or personal data. Personnel in departments that need further training could include:

1. **Human Resources**
   Rationale: personal data collected and processed by the organization related to EU employees
2. **Marketing**
   Rationale: GDPR direct marketing and profiling implications, as well as ePrivacy Regulation implications
3. **Customer Service**
   Rationale: employees interacting with data subjects need to know how to interact with them and what information is allowed to be collected (ex. Front desk employees at hotel, travel agents, reservations, etc.)
4. **Customer Support**
   Rationale: any personnel collecting information from data subjects to solve issues will likely need to identify and authenticate those data subjects, as well as collect information related to the identified issue which could include personal data (ex. help line)
5. **Privacy and Compliance**
   Rationale: will need advanced training compared to the rest of the organization in order to lead privacy efforts

Getting Started

- Familiarize yourself with the chapters and articles in the GDPR program. Schellman has additional content beyond this white paper shared through blogs and recorded webinars.
- Understand how and where your organization ingests, stores, and transfers European personal data.
- Assess how privacy mature (or immature) your enterprise is.

Contact Us Today

Schellman offers several competitive differentiators for organizaions looking to align themselves with the GDPR. We are the first CPA firm that is 100% independent with no consulting agenda. We also offer organizations the opportunity to consult with our distinguished subject matter experts:

Chris Lippert
Privacy Technical Leaders
CIPP/E, CIPP/US, CISA, CRISC, CCSK

Kevin Kish
Privacy Technical Leaders
CISA, CIPP/E, CCSK, HITRUST

For more information or to contact us about your GDPR initiatives, go to www.schellman.com/gdpr


schellman