HFTP®
Hospitality Financial and Technology Professionals

EU General Data Protection Regulation (GDPR)

Compliance Tools for the Hospitality Industry

JOB DESCRIPTION:

Hospitality Data Protection Officer

This document highlights the role and qualities of a hospitality data protection officer. It can be used as a guideline for an internal recruitment, the expansion of an existing position or the recruitment of a third party to assist in the compliance for the GDPR.

This description was developed by the HFTP Hospitality DPO/GDPR Task Force. The task force is a group of 23 hospitality industry experts tasked with developing hospitality-specific guidelines to assist with preparation for GDPR compliance.

Learn more about HFTP and the HFTP GDPR/DPO Advisory council at **www.hftp.org**.

Job Description: Hospitality Data Protection Officer

EXECUTIVE SUMMARY

- The General Data Protection Regulation (GDPR) applies broadly to a vast array of organisations. The GDPR mentions that the extent of data protection expertise required of any organisation ought to be consistent with the level of that organisation's data processing sophistication.
- 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.
- The regulation identifies three (3) cases that necessitate the designation of a DPO and one of these cases would apply to organisations whose core activities "require regular and systematic monitoring of data subjects on a large scale," which would include companies in the hospitality sector.
- It is implied that designating a DPO is required for multinational, as well as publicly traded companies. Reporting to the executive management level, the DPO is a compliance officer, whose main duties are to protect data subject's rights by ensuring that an organisation fully complies with all GDPR principles. This includes privacy by design and by default, privacy assessments, and that the responsibilities of controllers and processors are adequately met. They are also an organisation's personal data advocate, involved with all issues relating to the protection of personal data. Furthermore, they must have access to all aspects (i.e. nature, context, scope, purpose) of data processing.
- As much as multinational companies might have the resources to appoint an internal DPO, this would be quite an expensive step for smaller companies in the hospitality world. In that case, it must have internal practices in place to respect the GDPR requirements and to ensure that some of the attributes requested for a DPO's position are being taken care of by existing roles. The key criteria for the DPO appointment is independence in the exercise of his/her duties and absence of conflict of interests. Nothing prevents the DPO to be organically attached to any of the existing divisions within an organisation.
- An external provider could provide a DPO service, ensuring that all GDPR requirements are fully covered. The company remains responsible for compliance with GDPR and must be able to demonstrate compliance.
- A DPO function needs to be conversant, amongst other qualities, with:
  - » Knowledge and understanding of GDPR requirements; awareness of programs related to hospitality such as PCI DSS compliance and local laws related to information security;
  - » Sound understanding of and familiarity with information technology operation and infrastructure (general design and functions of programs, platforms and applications, and how they impact personal data processing), and information security practices and audits;
  - » Knowledge of the hospitality business sector and of the employers' organization;
  - » Sufficient understanding of personal information (guests, associates/employees) processing operations carried out, as well as the information systems, and data security, data breach management, and data protection needs of the employer, storage of information; and
- It is a duty of the controller or processor to ensure that there is no conflict of interests in the appointment and/or exercise of the DPO functions. It is therefore an obligation to ensure such absence of conflict. DPOs should be free from conflicts of interest, they cannot hold a position with the organization that leads them to determine the purpose and the means of the processing of personal data or that otherwise creates a conflict. The position must be independent and a separate position from the CIO, CMO, COO and/or CFO.

This document highlights the role and qualities of a **hospitality data protection officer**. It can be used as a guideline for an internal recruitment, the expansion of an existing position or the recruitment of a third party to assist in the compliance for the GDPR.

Very clearly, the expectations the GDPR underlines as being part of the duties of the controller and/or processor are:

- Involvement in all matters relating to privacy and data protection;
- Providing resources for the performance of his/her tasks; and
- The DPO should report to top management and should not be influenced by anyone in his decisions. Equally he cannot be dismissed for performing his tasks.

JOB DESCRIPTION

Scope of Position

The DPO is an organisation's personal data advocate, involved with all issues relating to the protection of personal data. They must have access to all aspects (i.e., nature, context, scope, purpose) of data processing.

The DPO is responsible for internal practices in place to respect the GDPR requirements and prove compliance with the regulation.

The rules governing the function of the DPO should be part of and be included in the data management policies of the organisation and as such should be drafted by a collective data management group.

Main Duties and Responsibilities

The GDPR highlights some of the qualities of a DPO which includes as a prerequisite a total independence towards the creation, processing and controlling of data flow and data usage, therefore avoiding any conflict of interest. Without independence the tasks of the DPO cannot be fulfilled. The degree of independence is a prerequisite of the function.

The DPO role for the hospitality industry can be performed by an individual, a team or a third party with clearly recognised tasks and identified responsibilities. In case of vacancy, the company must ensure that the vacancy notice for the position of the DPO or the service contract is sufficiently precise and detailed to avoid conflict of interests with other departments.

- Inform, advise and issue recommendations to the company regarding GDPR compliance and the notion of guest (or employee) consent in an independent manner. The Act 39, 1(a) clearly indicates that the role of the DPO is to inform and advise on how to carry out all processing operations: from what is the legal basis of the collection to the principles of the data collected, retention periods, appropriate security, etc. For example, in some cases, consent will be required. In other cases, consent may not be the best basis for collection. The legitimate interests of the company may be better suited.
- Advise the controller/processor regarding:
  - » Whether or not to carry out a Data Protection Impact Assessment (DPIA).
  - » What methodology to follow when carrying out a DPIA.
  - » Whether to carry out the DPIA in-house or outsource it.
  - » What safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
  - » Whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

- Records of data processing activities in accordance with Article 30 are not a specific task of the DPO. They are the responsibility of the controller, but they can be assigned to the DPO. What these records must contain are not references to specific applications and data management software. They rather consist of documentation on the name and details of controller and DPO, purposes of processing, categories of data collected and of data subjects, recipients of the data, transfers of data outside the EEA, storage periods and description of security measures.

  Maintain the record of data processing operations included in all aspects of the hospitality operating environment:

  a. System information security including (but not limited to) credit card processing, employees' data, general emailing system, data storage, PMS, point of sales, CRM, marketing, website, etc.
  b. Website reservation booking page
  c. Guest registration form
  d. Spa registration form and consultation form
  e. Guest preferences
  f. Loyalty programs
  g. Website email subscription
  h. Online marketing messages
  i. Website cookies
  j. HR/payroll system
  k. Recruitment process and retention of CVs
  l. Use of third party platforms of applications etc.

- Analyse and document processes and procedures of data flow management.
- Document all decisions taken consistent with or contrary to the DPO's advice and legal grounds confirming reasons for such decisions.
- Answer any request for access to the data by the data subject, as well as the exercise of any of data subject rights (rectification, erasure, restriction of processing, portability, right to object) and liaise with authorities in case of a data breach or other incident when required.
  - » Create and document an emergency response plan in case of GDPR breach or related complaint.
- Review of vendor contracts and ensure that all contracts will conform with GDPR.
- Review of employment contracts or contracted labour agreements to include an appropriate GDPR clause.
- Stay current with:
  - » Ongoing training
  - » New guest technology
  - » Hospitality trends
  - » Security and trends
  - » Legislation
- Training and awareness:
  - » Create a training plan to ensure wide knowledge of GDPR principles; and
  - » Foster a personal information data protection culture within the organisation and help to implement essential elements of the GDPR, such as:
    - › The principles of data processing
    - › Data subjects' rights
    - › Data protection by design and by default
    - › Records of processing activities
    - › Security of processing
    - › Notification and communication of data breaches.
- Ensure that no conflict of interest appears between the function of DPO and the tasks at hand by including safeguards in the internal rules of the organisation.

Standard Hotel Management Competencies (as per hotel company requirements)

- Expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR
- Experience in data protection program management commensurate with the sensitivity, complexity and amount of data the employer processes
- Integrity and high professional ethics
- Ability to handle information and business affairs with secrecy and confidentiality as appropriate
- Demonstrated leadership and project management experience
- Ability to communicate effectively with the highest levels of management and decision-making within the organisation
- Privacy Certificates/Certifications or Law Technical masters, familiarity with privacy and security risk assessment and best practices, privacy certifications/seals, and information security standards certifications such as for example PCI DSS, ISO 2007:

	Privacy Certificate/Certification Examples	**Focus**
CIPT®	Certified Information Privacy Technologist	Privacy
CIPM®	Certified Information Privacy Manager	Privacy
CIPP®	Certified Information Privacy Professional	Privacy
CISSP®	Certified Information Systems Security Professional	Security
CISM®	Certified Information Security Manager	Security
N/A	Privacy and Data Protection Foundation	Privacy
N/A	Privacy and Data Protection Practitioner	Privacy

- Sound understanding of and familiarity with information technology operations and infrastructure, and information security practices and audits
- Ability to communicate effectively with data subjects' data protection authorities and other controllers and processors across national boundaries and cultures
- Adequate self-awareness and confidence to acknowledge knowledge gaps and seek to fill them from reliable sources
- Knowledge of the hospitality business sector and of the employers' organisation
- Sufficient understanding of personal information (guests, associates/employees) processing operations carried out, as well as the information systems, and data security, data breach management, and data protection needs of the employer, storage of information