Institute of Hospitality

Management Guide

Get ready for the General Data Protection Regulation

Introduction

Despite Brexit, businesses cannot ignore the new data protection regime originating from Europe as it will come into law in the UK on the 25 May 2018 and you need to get ready for it now.

Although the EU General Data Protection Regulation (GDPR) does not fully come into force until May next year, it is expected to be in advance of the Brexit timetable, and because of its far-reaching effects, businesses are strongly advised to begin preparations for its implementation now.

In respect of employee personal data, the UK government is permitted to add more specific rules concerning the data of employees and it remains to be seen if and to what extent they will add domestic rules.

Warning from the Information Commissioner

Elizabeth Denham, the UK's Information Commissioner, has already issued a warning to business not to delay in preparing for "the biggest change to data protection law for a generation". Denham says: "If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance. But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit."

Companies that fall foul of the new GDPR will risk fines of as much as €20 million or 4% of their annual worldwide turnover, whichever is higher.

Hospitality and leisure focus

For businesses in the hospitality and leisure sector there are three significant areas that we would recommend are looked at carefully now so that you are prepared; firstly your legal basis for data retention and processing; secondly how you process such personal data and deal with subject access requests; and lastly how you will comply with the new accountability principle.

1. Data retention and processing – the lawful basis

For data processing to be lawful under the GDPR you will need to have a lawful basis. There are numerous potential bases for processing data under the GDPR but in the hospitality sector the following would be the most likely:

- Consent;
- Necessary to perform the contract or to take steps to enter the contract with a data subject;
- Necessary to comply with a legal obligation (and with "special categories of data" this is likely to be to comply with employment law or for example the antiquated *Immigration (Hotel Records) Order 1972 (as amended)* requiring guests to complete registration cards); or
- Necessary for legitimate interests of the controller and does not override the interests of the individual.

Consent is arguably the most likely legal basis in the hospitality sector and would be needed for instance for mailing lists, selection processes concerning job applicants and HR records. Businesses within the hospitality and leisure sector will already hold significant amounts of personal data, including customer personal data for the purposes of marketing, managing bookings and

registration, employee data for the purposes of payroll, sickness absence reports and holiday reports.

The GDPR includes heightened obligations compared to the existing UK Data Protection Act (1998), in particular regarding consent. Silence, pre-ticked boxes or inactivity will no longer constitute consent; consent must be freely given, specific, informed, unambiguous and there must be some form of clear affirmative action. If you retain any personal data on individuals you should ask yourself these questions:

- Have we obtained consent from each individual to use their details (e.g. email, address, telephone number)?
- Is their consent in a separate document to other terms and conditions?
- Are there simple ways for people to withdraw their consent?
- Do we use more than pre-ticked boxes or reliance on a party not unsubscribing as consent?
- Can we evidence the consent obtained?

If the answer to any of these questions is no, consent has not been freely given. To be compliant with the GDPR you will need to contact each individual to obtain their express consent to use their personal data going forward and keep a record of their consent to use as evidence. Alternatively you will need to justify the processing of their data under the other three grounds listed previously. Given the time changes are likely to take, it's wise to prepare your business now and consider how you will comply.

2. Employee and customer data – how you process and control personal data

The GDPR will impact on how you process and control the data of your customers and employees as follows:

- The £10 fee for a Subject Access Request (SAR) will no longer be permitted and there will be only limited circumstances where a reasonable fee can be charged.
- There is the added concept of transparency, which, for instance, means if an employee asks, you would need to explain how you approached their SAR.
- Unless a SAR is considered complex, businesses will generally have a month to comply with a SAR. Although you will be able to refuse or charge for requests that are manifestly unfounded or excessive.
- Of particular note, the exemption relating to legal privilege currently permitted has not been repeated. Whether the UK concept of legal privilege will trump data protection rights remains to be seen.
- Subject to limited exceptions, decisions significantly affecting employees will not be permitted if made solely by automated processing. This may affect HR processes such as performance management triggers relating to sickness absence, and recruitment shortlisting. Individuals should be able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.
- Unless a personal data protection breach is unlikely to result in risk to data subjects, an employer will need to report any data protection breaches to the regulator (in the UK, the Information Commissioner's Office) within 72 hours if feasible, along with other requirements. If there is a high risk to an individual's rights and freedoms you will also have to notify those concerned directly in most cases.

3. New accountability principle

A particularly significant change to the existing UK Data Protection Act regime is the new accountability principle. The GDPR will require you to show you have complied with its principles eg. by documenting the decisions you take about a processing activity. Even if not in breach, compliance will need to be demonstrated. If your organisation has more than 250 employees you are subject to additional requirements.

How you should be preparing

It is therefore imperative that the hospitality and leisure business sector begins to conduct an audit of their mailing lists, retained personal data (including employees, customers and suppliers) and related policies and procedures now. We recommend you review and plan:

- Refreshing (if your current consent processes would not comply with GDPR) and obtaining future mailing list consents.
- How you will deal with subject access requests or requests for personal data to be deleted from employees and/or customer records. How easy would it be to find and delete the data with your current processes? Who would make the decisions on what to send or delete?
- Recruitment processes, collection of data and shortlisting processes.

- Management of sickness and attendance bonus data.
- Holiday and shift rostering, if automated.
- Your use of CCTV.
- An information audit to document what data you hold, where it came from, who you share it with and identify the future legal basis for processing it.
- Review your privacy notices to see what information needs to be added.
- How you will effectively detect, report and investigate personal data breaches.
- How you will document your personal data-related decisions and comply with the new accountability principle.
- Any staff training required.
- Whether a data protection impact assessment or the appointment of a data protection officer will be required.

This Management Guide was created by Jonathan Gray, Head of Hospitality, Pitmans Law. Jonathan can be contacted on:

D +44 (0)23 8083 7785

M +44 (0)782 594 0525

E jgray@pitmans.com

Further Resources

Pitmans Law provides city quality legal advice for corporate and private clients locally, nationally and internationally. Their well-established data protection practice offers advice into processes, documentation, breaches and more. They are currently running a GDPR email campaign, known as their ***Pitmans Point GDPR Specials***, to help clients get regulation-ready by providing legal insights, templates, processes and surveys. They are also hosting a ***seminar on 28 September*** to share the latest best practice. To find out more please visit: ***www.pitmans.com/expertise/services/corporate/data-protection***

The EU GDPR Portal is an online resource to educate the public about the main elements of the General Data Protection Regulation (GDPR). ***www.eugdpr.org/eugdpr.org.html***

The UK Information Commissioner's Office has a web page devoted to Data Protection Reform which includes some useful self-assessment tools. ***ico.org.uk/for-organisations/data-protection-reform***