GDPR: what it means to the hospitality industry

preoday

Contents

Introduction: data ownership matters

The digital revolution in hospitality is ushering in profound issues regarding data ownership and regulation. The trends are obvious and daunting to consider.

A recent report suggests that 40% of key customer demographic groups like 25 to 34 year olds prefer to use their smartphone to order food and drink than queue at the bar or wait for table service, with that number likely to reach 65%. And according to a Deloitte survey, hospitality customers increasingly expect engagement to be delivered directly to their mobile devices, with 70% of respondents indicating they look for apps that deliver personalised offers and convey a sense that a restaurant "knows them."

Many hospitality businesses are running from behind given how quickly digital has transformed the industry, and no doubt everyone in the industry is mindful of the wasteland of retailers who failed to understand what was happening and respond quick enough to the digital tidal wave.

70%

of consumers want apps that deliver personalised offers - so data ownership is critical

Contents

Get in touch
for a FREE demo
preoday.com

Introduction: data ownership matters

Digital – the key to business survival

While adopting a digital strategy has become an imperative for hospitality businesses, the considerations go well beyond mere business survival. Digital hospitality solutions such as digital ordering present both opportunity and obligation. On the opportunity side, data ownership offers businesses with compelling value propositions.

Understanding who your customers are and their behaviours allow businesses both to engage with existing customers to build loyalty but also develop more effective marketing campaigns to acquire new customers. In today's digital-centric world, it is no surprise that customer data is increasingly one of the key assets by which companies in all industries are valued. Gartner itself recommends that organisations apply infonomics principles to their customer data by managing it with the same discipline as any other corporate asset.

45% **of hospitality businesses believe that the GDPR is not relevant to their sector – they are wrong**

Who owns your data?

But do you own your customer data? That may very well depend on commercial agreements you enter into with service providers offering digital solutions to hospitality. If you partner with an aggregator like Just Eat, you may not own the customer data, Just Eat does and your rights to data will likely be very limited. If you partner with a provider directly to offer your own app with a digital order feature, what you own or have rights to might still be unclear.

And new regulations set to come into effect next year have sweeping implications for data ownership and obligations that hospitality businesses will have to confront. The General Data Protection Regulation (GDPR) will become law as of 25 May 2018. Are you prepared for GDPR and the obligations it imposes on how customer data is collected, used and protected? A recent study suggested that nearly half of the businesses that will be subject to the GDPR regulations won't be. And a separate study of the hospitality industry found that 45% of the respondents believe the GDPR will have no impact as it's not relevant to their sector.

Make no mistake, the GDPR applies to hospitality businesses, the implications of the regulation are far-reaching, and the time to act is now.

Contents

General Data Protection Regulation overview

The GDPR was designed to modernise and unify data protection rules, enabling individuals to better control their personal data while benefitting businesses with clearer guidelines and reinforced consumer trust. The following is an overview of the new regulation:

Personal Data

The GDPR, like the existing EU Directive today and – indeed – any data protection law worldwide, protects "personal data" and, accordingly, it becomes important to understand what in fact constitutes personal data under applicable regulation.

Personal data is defined in both the Directive and the GDPR as any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

There are two key differences, however, with the GDPR. First, the GDPR makes clear in Recital 30 that personal data includes online identifiers and location data – meaning IP addresses, mobile device IDs and the like are all personal and must be protected accordingly.

The GDPR also introduces a new concept of "pseudonymisation" – personal data that is transformed in a manner (like hashing or data swapping) such that it no longer directly identifies an individual without the use of additional information.

Pseudonymous data, while still subject to certain requirements as personal data under the GDPR, provide organisations with added flexibility of use and reduced burdens, including exemption from the need to comply with data subject access, correction, erasure and data portability requests.

General Data Protection Regulation overview

Controllers and Processors

Since the GDPR applies to "controllers" and "processors" of personal data, it's important to understand what these roles are. According to Article 4 of the GDPR, different roles are identified as indicated below:

Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"

So, the organisations that determine the means of processing personal data are controllers, regardless of whether they directly collect the data from data subjects. For example, a bank (controller) collects the data of its clients when they open an account, but it is another organisation (processor) that stores, digitises, and catalogues all the information produced on paper by the bank. These companies can be datacentres or document management companies. Both organisations (controller and processor) are responsible for handling the personal data of these customers.

Keep in mind all EU organisations are controllers and likely processors since they collect and/or store the personal data of their own employees provided they're European citizens; therefore, all organisations are responsible for processing this data within the GDPR. The only question becomes: are you also subject to the GDPR with respect to personal data of your customers as a controller and/or processor?

General Data Protection Regulation overview

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You will be subject to regulation under the GDPR, as you are today under the Directive, since you are holding and processing personal data. The GDPR does cast a wider net than the current Directive, applying to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Consent

If you want to collect, store and use personal data, then you should assume you will need to obtain "consent", and the rules governing consent under the GDPR are more restrictive. Where the Directive allowed controllers to rely on implicit and "opt-out" consent in some circumstances, the GDPR requires the data subject to indicate agreement by "a statement or a clear affirmative action."

Affirmative action signalling consent may include ticking a box on a website, "choosing technical settings for information society services," or "another statement or conduct" that clearly indicates assent to the processing. "Silence, pre-ticked boxes or inactivity," however, is presumed inadequate to confer consent.

Consent: The data subject must indicate agreement by "a statement or a clear affirmative action." Affirmative action signalling consent may include ticking a box on a website, "choosing technical settings for information society services," or "another statement or conduct" that clearly indicates assent to the processing.

General Data Protection Regulation overview

Other important elements of consent under the GDPR include:

- The controller must not simply obtain consent, it must also be able to demonstrate that the data subject has consented to processing of his data, meaning that records will need to be kept for consent to be verifiable (Article 7);
- Requests for consent in the context of a written declaration or that are pre-formulated must be presented in an intelligible and easily accessible form, using clear and plain language and (in the latter case) not including any unfair terms (Article 7);
- Requests for consent made by a data controller using electronic means must be clear, concise and not necessarily disruptive to the use of the service for which it is collected (Recital 32);
- The data subject must be able to withdraw his or her consent at any time and the process for withdrawing consent must be as easy as that for giving consent (Article 7); and
- The controller must be able to meet the same standards of consent for any personal data previously collected, stored and used prior to the implementation of the GDPR, meaning for instance if the data was obtained by an opt-out method, the controller cannot use the personal data going forward unless and until the GDPR standards are met for that personal data (Recital 171).

General Data Protection Regulation overview

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities and implement appropriate security measures.

You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Be aware, should the outsource data processor breach obligations under the GDPR, the data controller can be held liable for penalties.

Fines and Enforcement

Fines under the GDPR for noncompliance have increased dramatically, indicative of a shift in attitude towards the importance of data protection and data security within the EU.

And violations of obligations related to legal justification for processing, including consent data subject rights, and cross-border data transfers, may result in penalties of the greater of 20 million Euros or 4% of the entity's global gross revenue.

Regulators may issue penalties up to or equal to the greater of 10 million Euros or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.

General Data Protection Regulation overview

Data protection officers

Data protection officers are already a feature of the data protection regime of certain EU member states, like Germany, though new to the UK. The GDPR introduces a uniform requirement for certain controllers and processors to designate a data protection officer, notably if their core activities consist of processing which, by its nature, scope or purpose, requires regular and systematic monitoring of data subjects on a large scale.

The data processing activities of the hotel brands, including their membership programmes, are likely to trigger the requirement to appoint appropriately qualified data protection officers. Businesses need to assess whether they will be subject to this additional administrative requirement.

Does my business need a data protection officer (DPO)? DPOs must be appointed in the case of: (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data (Art. 37). If your organisation doesn't fall into one of these categories, then you do not need to appoint a DPO.

Data protection by design and by default

Organisations will have to think harder about privacy and be proactive with regards to its operations and data management. Article 25 requires that organisations assess and implement appropriate technical and organisational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects — data protection by design.

In addition, organisations must put in place mechanisms to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation, data protection by default, includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

Contents

General Data Protection Regulation overview

Breach & notification

Under the GDPR, a "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

While the definition of a personal data breach has not changed in any meaningful way under the GDPR, what organisations must do should a breach occur will change dramatically with the GDPR. Currently, there is either no general obligation to notify or minimal sanctions for failing to do so. Under the GDPR, organisations have explicit notification obligations. In the event of a personal data breach data, controllers must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

And under Article 34, should the controller determine that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals," it must also communicate

Exceptions to requiring businesses to notify data subjects

The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances:

- The controller has "implemented appropriate technical and organisational protection measures" that "render the data unintelligible to any person who is not authorised to access it, such as encryption";
- The controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise;
- When notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

Businesses will need to assess their internal processes to ensure that appropriate procedures are in place to detect, investigate, report and document data breaches and to manage the fall-out from such reporting. As mentioned above, fines for failing to comply with the articles relating to security and data breach notification are up to 10 million Euros or 2% of annual worldwide turnover, potentially for both the controller and the processor.

General Data Protection Regulation overview

Greater rights for data subjects

Ultimately, the GDPR should be viewed as clarifying that personal data is owned by the data subjects themselves. This is reflected throughout the regulation in terms of protections and controls afforded data subjects including:

Article 13 and transparency — requiring various disclosures when data is obtained

Article 15 and subject access rights — information must be provided to data subjects if requested within one month

Article 16 and right to rectify — inaccurate or incomplete data must be rectified

Article 17 and right to erasure — data subjects have right to have data erased

Article 18 and right to restriction of processing — right to restrict processing in specific circumstances

Article 20 and right of data portability — data subjects may request to receive or have transmitted to another controller all personal data

Article 21 and right to object — data subjects may object to processing of data, requiring controllers to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds”

Article 22 and right not to be subject to automated decision taking, including profiling

Contents

What this means for hospitality businesses

Everyone must be compliant

It's safe to assume that GDPR applies to your business. Given the definition of "personal data", even simple direct marketing activities would fall into the category of "data controller" for which GDPR applies, such as newsletter signups, giveaways and the like. This means your hospitality business must ensure broad compliance with all GDPR requirements starting with implementing an "opt-in" based consent moving forward and for any personal data obtained previously re-establishing data subject consent consistent with the new requirements (assuming you historically used opt-out consent) or deleting and no longer using this data.

With respect to online or app ordering systems, as a practical matter, whether you work with an aggregator or offer your own online/mobile app, you will still need to comply with the regulation. That said, GDPR will significantly restrict rights that hospitality operators will have to any customer data when working with third party apps.

What this means for hospitality businesses

What happens if you use an aggregator

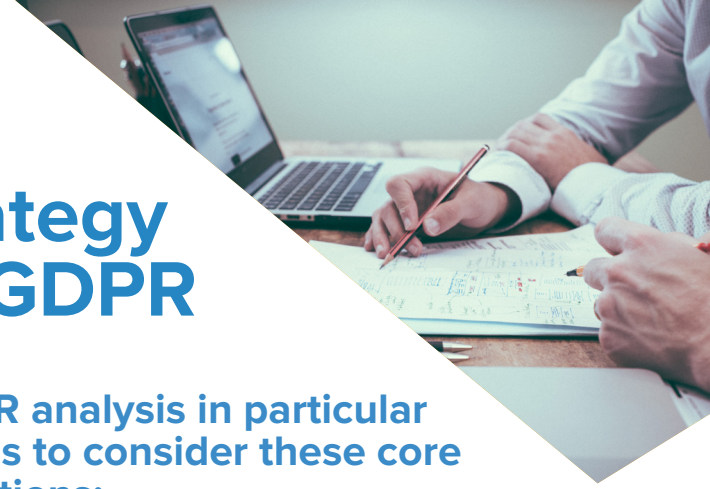
Under the GDPR, aggregators will be the data controller, and while hospitality operators may be granted limited rights as data processors, they will be restricted to use of the data based on the written instructions and need for use of the data as a processor for the aggregator. Ultimately, this means that hospitality operators may not use the data for any other purpose. In addition, the operators themselves will be subject to regulation under the GDPR, meaning broad compliance to various obligations and liability for failure to comply.

Accordingly, hospitality operators working with aggregators will inherit lots of obligations and no real benefit to customer data.

The only way around this would be for hospitality operators to move off the aggregator platform and create a direct customer relationship by launching their own online or app ordering solution.

This will ensure that, come May 2018, the hospitality operator will be the data controller and, accordingly, have greater usage rights and control of its customer data.

The GDPR will have a broad impact on the hospitality sector. The regulation mandates will require operational changes across the organisation, both to systems and personnel. While the obligations are significant, the regulation presents the opportunity for hospitality businesses to think more critically about its digital strategies. Who owns, controls and processes customer data is important to understanding compliance with the GDPR but also crucial to adapting to the digital tsunami that is transforming hospitality.



Developing a data strategy in preparation for the GDPR

Organisations should approach GDPR as an opportunity to develop a holistic data governance and information management strategy. Consider the gap between what data organisations have today and the information or business advantage they want to have tomorrow as a 'data delta'. Achieving digital transformation can be a huge headache because this delta exists within most organisations, and yet it must be bridged if companies are to truly embrace digitalisation and survive. GDPR compliance is a specific example of a data delta that needs to be crossed and the best way to approach it is with tried and tested data management practices.

Organisations should consider the following principles when developing their holistic data strategy:

- **Data must be governed and owned**
- **There must be an agreed description of the data**
- **Data quality must be defined, measured and managed**
- **Principles of access need to be established, addressing each aspect of the data lifecycle, storage, privacy and security**
- **How data is used and shared needs to be agreed as well as how systems are integrated**
- **The organisation needs to determine which data needs to be controlled, how and by whom, so that business applications can be successfully implemented**

GDPR analysis in particular needs to consider these core questions:

- What personal data does my business hold?
- Why does my business hold this? (For which processing activities purposes?)
- Does my business have specific consent and have I registered any objections?
- How will I continue to monitor and action consents and objections?
- Is my business upholding the rights of the data subject?

For compliance purposes, organisations must continually manage and update their data collection systems. It is an iterative process, not a one-off activity and therefore it is not merely answered by a technology implementation. **Organisations will need to look at the three core areas of process, people and technology right across the organisational landscape.** This is an integral part of having a defined strategy for information management and a strong grip on data governance.

Developing a data strategy in preparation for the GDPR

Viewed from another lens, organisations should consider the following questions:

- **How to convince customers to keep giving data and consent to the data activities it wishes to develop?**
- **How to be compliant and minimise investment?**
- **How to create awareness, align workforce, prioritise efforts, while minimising IT impact?**

Involve stakeholders

Harmonising this is no small task but the key will be participation of the right stakeholders. The goal is to facilitate involvement of the impacted departments and to find compliant solutions without obstructing business as usual. Therefore, including the right stakeholders will allow you to find the right balance between compliance, operational excellence and customer expectations. This requires, of course, appropriate project management skills to align all stakeholders while keeping an eye on the regulations.

Keep customers comfortable

Besides compliance and operational excellence, it will be important to keep customers comfortable with the data processing you envision. Customers are increasingly aware of the value of their data while being concerned with their privacy. Research has shown that customers are open to grant you their data consent, as long as they receive sufficient value in return and have the assurance they can adjust their preferences along the way.

Contents

GDPR preparedness

The U.K. Information Commissioner's Office (ICO) has published a list of 12 steps organisations can take to begin preparing for GDPR:

1. Awareness - You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information You Hold - You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating Privacy Information - You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' Rights - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject Access Requests - You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Legal Basis For Processing Personal Data - You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7. Consent - You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8. Children - You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

GDPR preparedness

9. Data Breaches - You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection By Design and Data Protection Impact Assessments - You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11. Data Protection Officers - You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

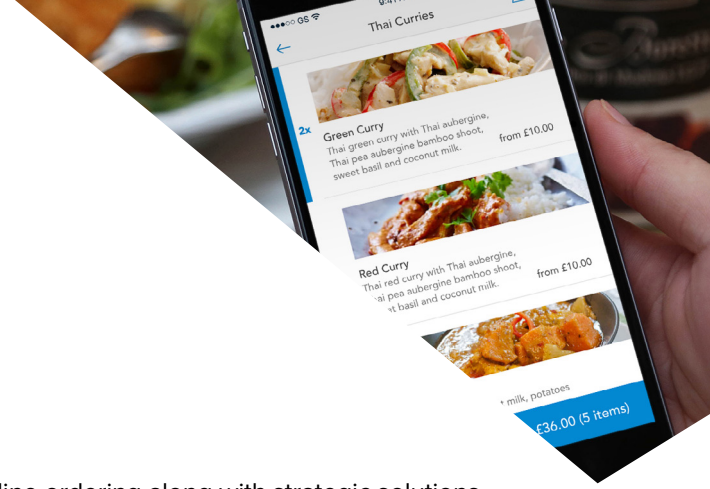
12. International - If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Given the strategic importance of data and the potential impact of the GDPR broadly on information management systems and governance, organisations should undertake GDPR preparedness like any critical project, with a defined project plan and appropriate resources allocated to execute.

Contents

Get in touch
for a FREE demo
preoday.com

About Preoday



Who we are

Preoday builds bespoke e-commerce platforms offering mobile and online ordering along with strategic solutions such as GDPR compliancy services. Preoday enables hospitality businesses to offer branded online and pre-ordering facilities to customers purchasing food, drink, merchandise and making bookings. It provides a white-label service to companies across the hospitality industry, from quick service restaurants and cafes, to theatres and stadiums. Preoday works both directly with hospitality businesses and partners including resellers, ticketing agencies, technology providers and food tech start-ups.

How we are supporting our clients with the GDPR

Preoday will do whatever is necessary to help clients mitigate shrinking margins and win the war with their competitors for control of consumer data and the consumer relationship. Many small and independent outlets do not realise the impact the GDPR will have on them and are fundamentally unprepared. The time to instil change is now as by May it will be too late to start tackling data rights and use.

There will be many casualties from unprepared restaurants and restaurants/venues that fail to understand and, more importantly, adapt quickly to the new paradigm and regulations. Preoday wants to ensure that its clients are not among them.

We have set up an advice line for businesses, GDPR@Preoday.com. We understand what the GDPR means for the hospitality industry and we are committed to supporting businesses and providing them with solutions to help them become GDPR-compliant. We would be glad to help you as we already help our clients. The time to act is now, get in touch today if you would like to find out more.