Guestline

GDPR

Are you ready?

Introduction

Due to the imminent arrival of General Data Protection Regulation (GDPR) on 25th May 2018, it's vital that all hospitality accommodation providers are making preparations now to ensure they are well and truly 'GDPR-ready'.

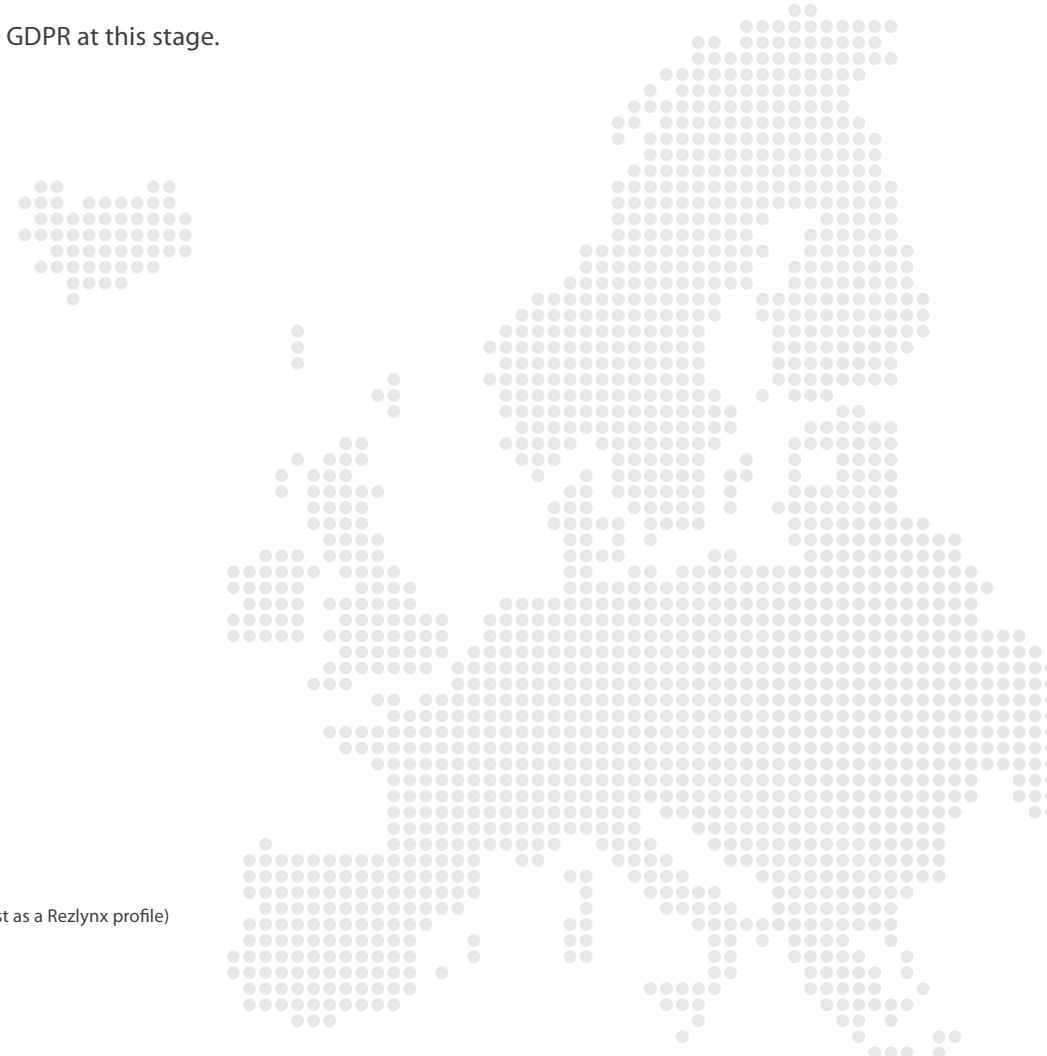
Data Controllers need to be making sure that they know what data exists, where it's held, who has access to it and how it's processed.

The key principal behind GDPR is that it has been designed to provide the data subject with more power on what information organisations hold and what it is being used for, thus empowering the data subject with much more control over the use of that data.

Comprehensive details on the GDPR and official guidance on its provisions are available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

What is GDPR?

- The General Data Protection Regulation (GDPR) requires any business that handles the personal data of EU citizens to ensure adequate protection is in place to prevent theft or misuse.
- Under GDPR, all consent requests relayed to data subjects must now be easy to understand, there will be no room for unnecessarily complicated language and content must be written in plain English.
- Consent must be just as easy to withdraw as it is to give - and data subjects now also have the right to be forgotten without delay.
- Bear in mind that GDPR extends not only to your guests but also to your employees, as you hold personal information on them.
- You are obliged to consider the rights of your data subjects, which is a main feature of GDPR as it grants people whose personal data is handled more rights than before across the EU.
- Brexit is not expected to impact GDPR at this stage.



NB: Data subjects are customers (e.g. a hotel guest as a Rezlynx profile) and employees.

0800 413 557 GDPR@guestline.com

What is going to happen?

As a Regulation (as distinct from a Directive), GDPR will apply directly in all Member States from 25th May 2018 without requiring any implementation into national law.

It introduces a new sanctions regime along with expanded and prescriptive requirements that will increase the regulatory burden on data controllers and, for the first time, directly impose data protection obligations and liabilities on data processors.

The emphasis is on accountability: not just complying with the law, but demonstrating compliance, including obligations regarding record-keeping, appointing data protection officers, and codes of conduct/certifications.

GDPR will not prevent you from marketing to your customers nor will it stop you from running your organisation; the purpose is to provide clarity on data structures and accountability.

What do you need to think about right now?

For the hospitality accommodation industry, there's a lot to be working on and it's vital that you are on track to ensure compliance.

- What data do you currently hold?
- What procedures are in place to deal with subject access requests (SAR) and deletion requests?
- Are your privacy notices up to date?
- Are your consent statements up to date?
- What processes do you have in place to investigate and report data breaches?

These are all questions that businesses need to consider now, as the countdown is on.

Suppliers

As a business, you should take stock of all of your suppliers, as you are likely to be using a number of data partners and platforms on a daily basis. You should also check your contracts with them and ensure they're providing clarity around the data they hold or process.

Typically, you may use any number of data partners on a daily basis. Look, for example, at your Email Marketing Databases / Pay Per Click Marketing / Property Management System / Online Travel Agents / Channel Managers / Booking Engines / Membership Systems / Social Media Marketing / Employee Management Systems / Recruitment Agents / CCTV and so many more – you are required to "think GDPR" and your responsibility is to ensure you know where your data is kept.

Personal identifiable information

GDPR requires you to be clear and transparent on how you handle PII (Personal identifiable information) and keep it secure and safe, what you do with the data, why you use it, when you will dispose of it and how you will grant access to any data held.

Data subjects have the right to be forgotten and erased from records and you must have a clear process in place on how to action these requests. All of these points will also relate to how you formulate your consent statements.

UK and EU

The GDPR will be relevant to you whether you have a UK-only focus or have operations in the EU and/or with EU customers. This is key as it is your responsibility to understand how the regulations affect your customers and employees whose data you hold.

Key considerations

Consent - your customers and employees are data subjects; understand the rules around 'consent' and 'what the data will be used for'.

GDPR demands that data protection is structurally included in systems and processes from the beginning, by design and by default. This means that privacy must be a foundation for every action undertaken which involves the gathering and processing of personal data.

Data protection by default means that in the default settings of a particular product or service the strictest principles of data and privacy protection must be present.

Guidance from the ICO suggests that you are not required to automatically 'repaper' or refresh all existing DPA consents. But if you rely on individuals' consent to process their data, they say that you must make sure it meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented, only used for legitimate purposes and can also be easily withdrawn. If not, alter your consent statements and seek fresh GDPR-compliant consent, or identify an alternative to consent.

Personally Identifiable Information - what does this include?

Personally Identifiable Information (PII) is identified by the ICO as any data that could potentially identify a specific individual; any information that can be used to distinguish one person from another. This includes but is not limited to: Name, address, location, online identifier, health information, income, cultural profile and more...

They also advise that Personal Data cannot be further processed in a conflicting manner with the purposes outlined initially – for example, taking an email address at the time of enquiry/reservation and then using it, without additional consent, for email marketing purposes at a later stage.

Under GDPR, specific consents are now required for example for: email marketing, loyalty, (web) cookies etc. Consent under GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes.

Changes to fines and liabilities in the event of data breaches and data theft etc

Fines

Fines for infringements of GDPR obligations make data protection a key issue: these can be 4% of total worldwide annual turnover or €20 million if higher, for obligations deemed most fundamental; and 2% of total worldwide annual turnover or €10 million if higher, for other obligations.

Reporting a breach

If your organisation is unfortunate enough to experience a data breach, then under GDPR you would need to ensure that this breach is reported to all stakeholders and regulatory authorities within 72 hours of the breach being discovered.

Data Protection Officer

Under the ICO guidance, you will need to consider the appointment of a Data Protection Officer, checking whether the GDPR specifically requires you to appoint one. Article 37 of the GDPR details three specific cases where an organisation must recruit, hire and give responsibilities to a DPO if:

1. They're a public authority or body processing data (e.g. a hospital)
2. The core part of the business is the control and processing of data, and they do this on a large scale, with 'regular and systematic monitoring of data subjects'
3. They process large amounts of the special categories of personal data, as defined by the GDPR.

Your Key Steps to GDPR compliance (based on the ICO guidance)

01 Awareness

Is the hotel GM/senior management team aware that the current law is changing to GDPR and that it will affect the hotel's operations?

02 Information you hold

Organisations need to maintain records of all processing activities and the legal basis for processing such data.

03 Communicating privacy information

Organisations should review their privacy policies for both hotel staff data and for hotel guest data. Does your hotel policy adhere to GDPR? Think about hotel email marketing systems, loyalty systems/clubs, website lead forms, cookies for example.

04 Individual's rights

Procedures need to cover all the rights individuals have (both hotel staff and hotel guests), including how you would delete personal data or provide data electronically and in a commonly used format. You will need to provide information in a commonly used machine readable form, free of charge.

05 Subject access requests

Organisations should update policies and procedures in place to deal with subject access requests to ensure you can comply within the new one-month deadline.

06 Lawful basis for processing personal data

Review the legal basis for undertaking this processing of data. Look at the types of hotel staff and customer transaction data processing that you and third parties (suppliers of technology systems, membership systems, employee software, recruitment agents for example), undertake.

07 Consent

Where your organisation relies on consent, you should read the ICO guidance, as this legal basis is undergoing the most change under GDPR.

08 Children

Under the GDPR, for the first time, children's personal data will be specially protected where organisations are offering information society services directly to children. Organisations should ensure they have processes and mechanisms in place to verify the age of users and seek parental consent for children under 16.

09 Data breaches

In certain circumstances organisations will only have 72 hours from discovery of a breach to notify the relevant data protection authority of the breach. Organisations will also have the obligation, in certain circumstances, to notify data subjects directly if the data breach is likely to result in high risk to their personal data.

10 Data protection by design and data protection impact assessments

PIA's will be required where processing is likely to result in high risk to individuals, e.g. where rolling out new technology, where profiling occurs or where processing is conducted on a large scale. The ICO and the Article 29 Working Party have released guidance on this issue.

11 Data Protection Officers (DPO's)

Organisations should evaluate whether they need to appoint a DPO under the GDPR.

12 International

Where your organisation operates in more than one member state, you should identify the lead supervisory authority. For more information, please see the Article 29 Working Party guidance.

It is important to note that for Guestline customers - as the Data Owners under GDPR legislation - that they have ultimate ownership and control over how/when/where their data is used and Guestline therefore have no control or ownership over that data and the decision-making processes involved.

Guestline
Hospitality Software Solutions

About Guestline

Guestline's unique, cloud based suite of solutions for the hospitality industry increases revenue, streamlines operations and lowers costs.

Guestline provides end-to-end property management, channel distribution and digital marketing solutions to a range of hotel groups, independent hotels, serviced apartments, management companies and pub companies.

Fully integrated and cloud based, the solutions are easy to install and quick to deploy with low cost of ownership.

With offices in the UK, Ireland, Germany, The Netherlands and Thailand, Guestline's systems are used in 25 countries across 5 continents and enables properties of all sizes to achieve maximum occupancy at the most profitable rate.

Guestline House, Shrewsbury Business Park, Shrewsbury, SY2 6LG
0800 413557 +44 (0)1743 282300 GDPR@guestline.com **guestline.com**