GDPR – Advice for the Hospitality sector[1]

1) SITUATION

GDPR, what is it, and is it important to the Hospitality Sector?

The General Data Protection Regulations (GDPR) is a major overhaul of the EU data protection law. It comes into force on May 25th, 2018. It requires any business (including hospitality industry businesses) that handles personal data of a EU citizen to have adequate measures in place.

What is meant by "adequate measures"?

By "adequate measures" they mean data should be properly protected, and any theft or misuse of this data cannot occur. The EU citizen (the guest) also has specific rights on the data that you are holding about him. (see below)

Does GDPR only apply within the European Union?

No, it applies to data stored on EU citizens, wherever they are staying around the world. This impacts the entire hospitality sector, worldwide.

What if I am not compliant?

If a EU citizen files a complaint, the hotel may face some hefty fines. The maximum fine is set to 20 million Euros, or 4% of the annual global turnover (whichever is the greater).

2) HOW TO PREPARE in 13 STEPS

There are several steps that the hotel can take to properly prepare for GDPR. Some of them may already be in place. They are listed below.

2.1) Create awareness in the hotel.

Ensure all employees are aware of what is coming in 2018. There may already be excellent guidelines and procedures in place, for example your credit card information handling may be PCI compliant, but now the scope will be larger. Consider, for example, health club data or engineering intervention records which may hold personal data. An awareness session for the entire staff is a good starting point.

[1] Based on rules & regulations as applicable in Belgium

Buy-in of the hotel management team is also essential. There may be changes in procedures or systems, so all managers should be aware of GDPR, fully understand it, and be able to understand the impact on their department.

2.2) Create a "data-register"

You should be documenting which information you are holding, where it is stored, where it comes from, whom you are sharing it with, and if the guest has given his consent to you collecting all this data. This "data-register" will map all your data streams.

All processing steps should be recorded, and this may require the compilation or review of existing policies and procedures.

2.3) Communicate to your guests about your new privacy rules

Make sure you ask the guest for his agreement on giving you all required data, and document that agreement. This could be easily done on the registration card, or when checking-in on line. Adapt your legal statements and customer agreements to the new legislation. You will need to disclose for which purpose(s) you intend to collect data, and how long you will be keeping it.

2.4) Guests rights

The European guest has several rights, and you need to ensure he can exercise his rights, which include:

- The right of access to his data
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to transfer his data to another party
- The right to object
- The right not to be included in automated marketing initiatives or profiling

Many of those rights may already be in existence today.

2.5) Guest access requests

You will need to be ready to handle a guest request coming in about his rights. You are not allowed to charge for this service, and you have a maximum of 1 month to provide an answer. If you refuse a request, you must inform the guests about your reasons, and provide any details about the Privacy Commission and the name and contact details of your DPO (Data Protection Officer, more on this below), so that the guest understands how to file a complaint.

2.6) Lawful basis for processing guest data

While the hotel is collecting data, it can only do so if there is a lawful reason. You need to review and ensure all questions you are asking (on registration cards, online forms etc…) are absolutely required for you to process the guest. As an example, the departure date of a guest is a required piece of data. However, asking for the guest's birthday may be more difficult to justify.

2.7) Guest consent

It is important to review how you are obtaining, and recording the guest consent. He may be arriving via a travel agent, via a telephone reservation, or it may be a walk-in. All these cases need to be considered.

At all times, there must be a clear "opt-in" given by the guests. There cannot be any pre-ticked boxes where the guest agrees to give his data; opting in is never by default. Also consider how you will handle the case of a guest who withdraws his consent.

2.8) Children

There's an additional consideration for children under 16. Authorisaton to process a minor's data should be obtained from their parents or responsible adult. The hotel needs to prepare for this scenario.

2.9) Data breaches or theft

The hotel should be ready to detect, and remedy any data theft concerning personal data. The data register should be able to provide insight into which pieces of data are concerned.

Any incident should be reported within 72hrs to the Privacy Commission, for all cases where there is a risk that guest data may have been compromised.

By extension, this implies your network and storage systems should be up-to-date with the latest intrusion detection programs and should have successfully passed penetration testing.

2.10) Data protection by design, and Data Protection Impact assessments

For any new systems or major changes, it would be wise to keep the "Data protection by Design" in mind. Indeed, when discussing requirements for a new tool or procedure, you can already include the data protection principles, right from the design stage.

An Impact Assessment is required when major new technology is introduced, or significant upgrades are taking place on systems which contain personal data.

2.11) The Data Protection Officer

Within your hotel or company someone should be tasked to become the Data Protection Officer (DPO). Make sure this is someone who knows and understands the importance of personal data processing. This can very well be an additional task for an existing employee or manager.

It is mandatory to appoint a DPO when you are handling large volumes of personal data records, such as medical or criminal records. In a hotel, large amounts of credit card details are processed, so it is eminently sensible to have a DPO in place.

The DPO should always understand and be aware of all data flows in the hotel, and he should ensure that he has an updated data register at all times, in case any queries arise.

The name of the DPO should be mentioned on all privacy statements on any media. When filing a complaint, the guest will reference the DPO by name.

2.12) International and Group Hotels

If you are an independent hotel, this point does not apply.

For hotels with multiple properties, or in multiple EU countries, it is important to align the procedures, and to identify who is taking the lead (presumably the country or regional office) for the coordinated GDPR efforts. If you are present in multiple EU countries, it is required to identify a "main establishment", and also the country lead supervisory authority.

2.13) Existing Contracts

It is likely that for the processing of your data you are assisted by third parties or subcontractors. Make sure you are aware of who they are, and what your current contractual obligations are. It would also be an excellent opportunity to review these contracts to include any GDPR related aspects and ensuring the contractor is aware of his obligations under GDPR and that services or systems help you meet your GDR requirements.

3) MORE FAQ'S

Who is overseeing the introduction of these new regulations?

Every country has one central organisation to oversee the introduction of the new regulation. For Belgium this is the "Privacy Commission" (https://www.privacycommission.be). Any queries or complaints from guests will be addressed to them.

Who is responsible?

Ultimately it is you, the hotelier who is responsible. So, if any of the above points fail, and a guest files a complaint with the country authority, it will be addressed to you, and you will have to justify your actions to the Privacy Commission.

4) What if I need assistance?

Quality Hotel services can help you in several ways:

- Compile a comprehensive awareness campaign, tailored to your property
- Set up a "data-register" for you, or provide you with a workable template
- Making sure the necessary "consent" statements are included on all printed and electronic media where you collect guest data
- Recommend processes on how to obtain consent from guests, and children
- Ensuring your network and data storage devices are 100% safe and protected
- Design an "Impact Assessment Analysis" template document
- Compiling the job description and procedure manual for a DPO
- Compiling your "Data" supplier list, and reviewing/suggesting contractual amendments