GDPR ACTION PLAN

1 AUDIT

You need to identify what personal data you hold, where it came from and who you share it with.

This can be a simple paper audit (see document 1.1) or it can be in a spreadsheet with tabs for each department (under development).

2 RISK

Once you know what data you process, you need to identify where the risks lie. This can be included in the audit step but it is useful to take a step back and look at how data moves throughout your hotel.

Identifying potential problems now will help you shape what you do in each step after.

3 SECURITY

Now that you have identified your data and know the risks, you can look at the steps need to secure that data.

This applies to digital and paper files. Privacy by design is a legal requirement and you might complete a Data Protection Impact Assessment (see document 3.1) if you are making changes to your processes.

4 LEGAL BASIS

In order to complete your privacy notice in step 5 you need to know the lawful basis for your processing.

This might be consent, contract and/or legitimate interest amongst others.

Most hotels will rely on legitimate interest but you cannot use this for email marketing. More information in the next section.

5 PRIVACY COMMUNICATION

When you collect personal data you need to give certain information, such as your identity and how you intend to use the information.

Our Privacy Notice Toolkit (document 5.1) will help you write a privacy policy and will look at what legal basis to use.

6 POLICIES

When you have completed an audit of your personal data and identified (and corrected) any security weaknesses, you will need robust policies to help your staff process data correctly.

Our list of policies (document 6.1) is a starting point and we will be developing these further.

7 CONSENT

If you carry out email marketing, you cannot rely on Legitimate Interests as your legal basis. PECR regulations cover this in addition to GDPR. You need to have consent or what is called soft opt-in.

This does not mean dumping your existing contacts or asking them all for consent. See documents 7.1, 7.2 and the privacy toolkit 5.1.

8 BREACHES

Create a procedure to handle data breaches. This could be as simple as losing one customer credit card file.

Treat a data breach just like a first aid incident. Have a way to record it and a procedure to follow up.

9 REQUESTS

Customers and employees have new rights to request access to the data you hold on them. You will need to know how to respond to these requests and be able to action the request within one month.

Customers may also want to withdraw from marketing so you should make this easy and automated if possible.

10 REGISTER

Finally, if you are not already registered with the Information Commissioner's Office, do so now.

The process takes about 15 minutes and costs £35 per year (under review).

It is a criminal offence not to register under GDPR so don't ignore this.

Note: This is intended to provide an overview of GDPR and is not a definitive statement of the law.