GENERAL DATA PROTECTION REGULATION
An introduction and guidance for LHA members
These notes are intended as a guide, not as a definitive interpretation of the new Regulation. You are advised to take specialist advice should you wish specific guidance or support in respect of your own business

GDPR supercedes the existing Data Protection Act with effect from 25 May 2018. It further refines a lot of what is already in place and what businesses should already be doing with customer data and information.

It applies to anyone who processes (ie: does anything) , either as a controller (decides the what and how) or as a processor (undertakes activity for a controller), the personal data (ie: anything that can identify an individual) of any data subject (ie: an individual who is the subject of personal data). In essence, if you are capturing or recording details about enquirers or guests – however you record the information – GDPR applies to you; and you are almost certainly a controller.

GDPR requires that any information you capture is –
- Obtained with the consent of the individual;
- Collected for specific and legitimate purposes;
- Handled transparently, fairly, lawfully and in a secure manner;
- Relevant and limited to what is necessary for the purpose;
- Accurate and kept up to date;
- Kept for no longer than is necessary;

And that you are accountable for this (ie: you can demonstrate compliance)

GDPR requires that your data subjects –
- Give consent for whatever you want to do with their personal information;
- Know that you are collecting information about them and what you are doing/will do with it;
- Can obtain a copy of the information you hold about them;
- Can request that information is corrected, updated or deleted;
- Can refuse to let you process or profile their information

So what does this mean for the typical hotel, guest house, B&B, hospitality business...?

You must ensure that you have a robust and secure method of recording guest information, and you have appropriate trackable policies and systems to back that up
- *If you use an online database or list, is your computer system passworded, is the database file passworded, do you have good and up-to-date anti-virus and internet security software.*
- *If you have printed/written/physical lists or documents are they kept secure.*
- *Do you have an IT, Privacy and an Information Security Policy in place.*
- *If you use a third party (eg: an online booking system or calendar; or a payment system) are you satisfied that they demonstrate full compliance.*
- *Can you demonstrate the above*

You can only capture enough information needed to fulfil a contract (eg: a room booking) and you can only hold that information for the duration of that contract.
  - Technically this means you can only capture information that is necessary to make and fulfil a booking, and once a booking is complete you have to delete the guest's information.
- *You can get around this by advising guests (ideally in your Booking Conditions) that the first time they book you will create an account for them, containing their relevant information, making it easy to book on future occasions. An account can be used for multiple bookings, so you can hold a guest's details beyond a single booking.*
- *However, you need to decide – and make known to customers (usually through your Privacy Policy) - how long you will retain any information and why (ie: you could reasonably argue that information relating to bookings should be held for 6 years because on accounting requirements), but what about enquirers or other personal information that might not be relevant to a booking.*

A customer or potential customer has to give their consent for you to use any personal information they provide. Please note that consent now has to be given – the customer has to opt in – which is change from

the existing arrangement where it has been assumed consent is given unless a customer says otherwise and opts out. There is also now a distinction drawn between information used for (say) a booking and for marketing

- *You can reasonably assume that consent is automatically given with information provided to make a booking (as, obviously, without that the booking could not happen) BUT if you want to use that guest's details to market to them before/after their booking (or if they are an enquirer who hasn't booked) you MUST obtain their consent for this and be able to show you have that consent.*
- *Equally importantly, the same requirement will now apply for ALL existing individuals on your customer database. This means that if you want to market to your customer database (whether that is to encourage more bookings or just general marketing, you MUST contact everyone on your database and ask them if they want to receive marketing information from you. As noted above they have to opt in, so unless they respond with a positive request (and you can show that) you can no longer contact them.*
- *There is a general assumption going forwards that it should be as easy to remove consent as it is to give it.*

A customer or potential customer has the right to ask to see what information you hold about them, and for that information to be corrected, up-dated or deleted.

- *At first glance this seems sensible – after all, if a guest changes their address then why wouldn't we want to make sure that information is correct. However, a customer can ask for a copy of what information you hold, and you have to respond within one month. Such information could be bookings as well as personal information – how easily can you retrieve that information if you received a request.*
- *If you have passed information on to a third-party, then any request for correction or updating has also to be sent to that third party by yourself.*
- *If deletion is requested by an individual, then ALL information should be deleted..potentially including on any back-ups or archived records. How easily can you achieve this (and can you show that).*

Where you have a website or a web presence, you now have to ensure that all points at which personal information can be gathered comply with GDPR – this includes cookies and other visible touchpoints.

- *If there is no genuine and free choice then there is no valid consent. Cookies are now regarded as personal data. So if your website uses cookies, you MUST now obtain a positive action to demonstrate consent (and be able to show that, probably by recording IP addresses). Saying "by using this site you accept cookies" is no longer applicable, you must provide an opt-in – it is likely that website providers will come up with suitable options.*
- *You must also be able to accept "Do Not Track" browser requests – again it is likely that website providers will provide relevant options, but you should be aware of these issues.*
- *Removing consent has to be as easy as giving it, so in all cases your website has to have a way for individuals to delete their details or to unsubscribe.*
- *Privacy Policies will need to be updated to comply with the GDPR, particularly in respect of informing individuals about what information you are collecting, what you are doing with it, how long for, and how individuals can get data changed or deleted.*

Finally you need to have a procedure in place in case you have a data breach, whether this is hacking or physical theft of printed information. This exercise can help in identifying how management of data could be improved and made more secure within your business. Under GDPR any business or organisation suffering a data breach must advise the Information Commissioner's Office (ICO).

This all sounds horribly complicated and time consuming...

Although everyone is supposed to be ready for GDPR at the end of May, there is likely to be a short period of leeway (although there has been a two year preparation period already). Equally, it can be expected that the media and consumer groups will be looking out for easy cases to pick up. The key point is to be aware of your responsibilities and start to address those. By showing due diligence – that you are working on addressing the key points – then you have reasonable protection; sticking your head in the sand and hoping it will go away will not work. Do not get misled by companies offering to solve all your issues - look at the information on the ICO website and speak with your website designer or hosting company. LHA will also continue to provide guidance, information and good practice ideas on its website.