Are you ready for GDPR?

David Derbyshire, Chair of HOSPA IT Committee, addresses the elephant looming across the sector and beyond.

By now almost everybody in business has heard about the new General Data Protection Regulation (GDPR). LinkedIn is awash with articles and experts offering all manner of advice, reports and consultancy to advise you on compliance. While this short article can't offer you that, it will hopefully shine a light on some of the implications for the hospitality industry.

GDPR replaces the previous Data Protection EU Directive 95/46/EC, and harmonises it across the EU. It will replace the UK Data Protection Act (1998). Some of you may be wondering what the distinction is between a Regulation and a Directive. This is worth a brief explanation:

- Regulations automatically apply across the entirety of the EU.
- Directives require member states to create their own national legislation to accommodate the new law.

This distinction is important. It means that for the first time the law will consistently protect the personal data of EU citizens wherever they live or work within the EU, and importantly, outside the EU. This means that you and I as EU citizens are (at least in theory) protected even when staying in a hotel in the United States, China, or anywhere else on the planet.

The GDPR becomes law with effect from 25th May 2018. From this date, all organisations that hold or handle data that can identify any 'Natural person' (living individual) must comply. The penalties are high - far higher than the prior legislation, with financial penalties rising to a maximum 4% of annual turnover, or €20,000,000. For large organisations 4% could be a lot more than €20m, let alone the reputational damage that a data breach can cause.

So, what does this all means for hospitality? As HOSPA members learned during the recent IT Community event at the BT Tower (courtesy of our hosts BT Wi-Fi), GDPR is not just an IT concern, despite what some in your business may think. Admittedly, most data is held or processed by technology systems, but those filing cabinets full of old guest registration cards, spa medical consent forms, and kids' club registration forms should not be forgotten.

Neither should your HR files, disciplinary records, copies of pay slips, employee medical records, or any other form of physical records that contain PII (Personally Identifiable Information). What about old CCTV recordings? If you keep them for too long they could become a problem.

In practice, many of the processes currently in place for compliance with PCI and Sarbanes Oxley regulation, as well as the 'old world' data protection legislation will still be valid. However, GDPR offers greater protections to consumers, employees, and contractors than was previously the case. The EU designed the new regulation to bring data protection up to date, given the data revolution that human society has been through in recent decades. Whether we like it or not, most of us now have a substantial data footprint that simply could not have existed 20 years ago.

Consider some of the information that we collect now for our customers and employees: Name, date of birth, address, telephone numbers, email addresses, gender, ethnicity, bank details, loyalty club membership, guest preferences, and visa status. The list is almost endless - even online identifies such as IP addresses and cookies are in scope.

So how can you protect all of this data? There are some straightforward principles that you can follow to manage your compliance:

- Conduct a data mapping exercise (also known as a Data Protection Impact Assessment (DPIA). Understand all of the data that you hold and why. How accessible is it? Could you easily retrieve, delete, or amend it if somebody asked you to? How would you prove that you have complied with their request?

- Ask your suppliers how they are complying with GDPR. How are they managing your business data? They have a responsibility to treat it in a compliant way, but you are also responsible if they hold data on your behalf, to facilitate your business.

- Assess what data you retain for business need. This is an area where GDPR protects you as a data processor. You are entitled to keep data indefinitely if you can justify that it is necessary to conduct your business.

- If you do not need to retain data, why keep it? Once it is surplus to business requirement, or no longer required for any legal purpose (e.g. to meet accounting requirements, or employment regulations), get rid of it (securely!).

- When thinking about your business processes and systems, consider 'Privacy by Design'. For example, if you operate a CCTV system, how long do you need to retain recordings? Make sure you delete them automatically e.g. after 30 days, and that you can prove this if necessary. Securely archive your paper filing systems; and thinking of those archives, why do you really need them?

So, what are the rights that we will have as EU citizens under the new GDPR? I have managed to get this far without mentioning Brexit, but you should know that the UK will fully implement the law, which will then transition into whatever new legislation is created during the process of extracting the UK from EU legislation during the coming years.

Citizens have the following rights, which must influence how we design and manage the data that we handle in the industry:

- Right to know what information that is held about us.
- Right to access that data.
- Right to rectify anything that is found to be incorrect or out of date.
- Right to erasure of our data.
- Right to revoke consent (e.g. for marketing).
- Right of Data Portability (e.g. from one service provider to another).
- Right to be informed of automated decision making, use of AI to profile us (e.g. for sales or marketing purposes, or suitability for financial products or insurance).

These rights and protections must be kept in mind when designing business processes, selecting IT systems, or considering what information should be retained about any living person. There are also specific requirements with regard to minors (under 16) and to certain types of 'restricted data' (for example: race, ethnicity, sexuality, political beliefs, health information, biometrics).

Useful Snippets

There are other aspects of GDPR that larger hospitality organisations in particular need to be aware of, and which are considered Best Practice for all Data Processors:

- The appointment of a Data Protection Officer (DPO) is considered essential for large organisations to comply. This person needs to be able to operate without undue influence from the business, consequently must have seniority as well as a sound understanding of the Regulation, and of Information Management in general. The DPO role can be outsourced to a 3rd party, and this may be a more cost-effective solution for small/medium sized organisations.

If you spend any time researching GDPR you will come across the terms Data Processor and Data Controller. These are important roles to understand within the scope of the Regulation, particular where your customer or staff data is handed by a 3rd party (or if you happen to be a 3rd party service provider, handling data for another business).

- The **Data Controller** is the organisation ultimately responsible for the data. Controllers are responsible for ensuring Processors comply with any contractual terms for processing information.
- A **Data Processor** is any service provider that processes data on behalf of the controller, which they must do under a legally binding contract with the Controller, e.g. a cloud hosting provider offering data storage.

Some of the more challenging requirements of GDPR are those for data breach notifications. It is mandatory for an organisation to report any data breach to its supervisory authority within 72 hours of its discovery. In the case of the UK, the supervisory authority is the ICO (Information Commissioner's Office). In cases where there is a high risk to the rights and freedoms of the data subjects, they must also be contacted "without undue delay".

GDPR harmonisation rules can be superseded by local regulations, such as those relating to employment law or national security. For example, if a national regulation stipulates that employment data must be retained for 5 years after an employee leaves the company, it would not constitute a breach of GDPR to hold that data even if the employee had asked for all other records to be deleted.

In Conclusion

Nobody can be quite certain what the approach to enforcement for the GDPR will be. Clearly, it is critical to achieve and maintain compliance for all of the data that your business handles, but quite what compliance means is, to an extent, unknown.

Since there is no current case law, and no breaches, nor prosecutions have yet taken place within the scope of GDPR, there is little to help us understand compliance other than opinion, interpretation, and advice.

The authorities in the EU and the UK Data Commissioner have indicated that there will be a certain amount of lenience and understanding, so long as Data Processors can demonstrate their commitment to compliance, and efforts to improve on any failings are evident. Much will be made of the first notified breaches and prosecutions that take place.

So watch this space - do your utmost to be compliant by May 25th, and if you need expert advice make sure you shop around, seek multiple opinions or information sources, and always keep at the back of your mind, "If this were my personal data, how would I like it to be handled?"