Hospitality Ulster

# WHAT IS ALL THE FUSS ABOUT?


## The General Data Protection Regulation

www.hospitalityulster.org

# Personal Data & GDPR


## What is personal data?

We would suggest that for most businesses, common sense will identify the data that you hold.

A hospitality business might, for example, hold the following personal data:-

a. Names, addresses and telephone numbers of customers who make reservations.

b. Credit Card details of customers.

c. Email addresses of customers.

d. CCTV footage.

It is important to note that it is not just customer personal data that must be protected. Businesses must also protect employees' personal data. Those on whom you hold personal data are known as "Data Subjects".

## The Legal Speak

**Personal data is defined in the new General Data Protection Regulations as;**

> any information relating to an individual or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

### What is the General Data Protection Regulation (GDPR)?

The GDPR is the "General Data Protection Regulation" which replaces the rules laid down by the Data Protection Act 1998 ("The DPA").

The DPA already puts the onus on businesses to protect personal data. The DPA, however, largely pre-dated the internet and modern information technology systems. The GDPR is therefore an attempt to update the law.

Breaches of the GDPR will be investigated by the Information Commissioner's Office ("The ICO").

# What is all the fuss about?


## Using Personal Data

Under the GDPR, you can only use personal data for the purpose for which it is collected unless the person (Data Subject) consents.

If, for example, you take an email address for a specific reservation then this cannot be used for future marketing purposes or for other separate services without the consent of the person (Data Subject). This consent should be recorded diligently.

The personal data cannot be passed to a separate business without the person's (Data Subject's) consent. For example; passing details to a supplier for direct marketing.

### Getting Consent

If you intend to use the personal data for a purpose other than it was given, you must get the consent of the person (Data Subject) to use their data for this additional purpose and record their consent.

Consent can be given by the person (Data Subject) electronically ticking a box however it **MUST BE "OPT IN"**. The commonly used system where the person (Data Subject) "opts out" is not compliant with the GDPR and is therefore unlawful.

Written or oral consent can also be given by the person (Data Subject) but in both cases a record of the consent must be kept. Where oral consent is given, a record detailing the date, name and the nature of the consent given must be made.

### Marketing Consent

Providing customers with news and offers from your businesses is a vital part of most modern business marketing.

As offering a customer an option to "opt out" of marketing communications after the GDPR comes into force will no longer be lawful, businesses now need to sell the benefits of "opting in" to customers in the same way they sell any of their goods or services.

The 'Opt in' message must now be part of your overall marketing strategy, selling the benefits of receiving regular news and offers about your businesses. However, "opt in" message must also fulfil the new GDPR legal requirements and not be so obscure or confusing as to undermine the persons' (Data Subjects') right to understand what they are "opting in" to.


## Holding Personal Data

In many ways the overall responsibility of businesses to protect personal data will not change. The GDPR does however make provision for the following:-

1. An increase in the fines that can be levied by the ICO.

   The maximum fine will be €20,000,000 Euros or 4% of a business' turnover (whichever is greater).

2. A requirement that a personal data breach MUST be reported to the ICO if it is deemed to put the rights and freedoms of the Customer at risk.

   This means that many personal data breaches can no longer be "swept under the carpet". As such the need to take action to prevent breaches is even more important than before.

   Human error is inevitable and having a contingency plan is now imperative.

### What breaches of personal data need to be automatically reported to the ICO?

It is for businesses to make a decision on this but the GDPR offers guidance. It suggests that factors to be considered in determining whether a breach should be reported include:-

1. Breaches which may lead to identity theft.
2. Breaches which may to lead to financial loss.
3. Breaches which may lead to loss of confidentiality.
4. Breaches which may lead to loss of personal data protected by professional secrecy (e.g. medical records).
5. Article 9 of the GDPR includes specific special categories of sensitive personal data.

In deciding whether to report a breach a business will have to assess the likelihood and severity of the emotional distress to the individual whose personal data has been lost.

In addition, businesses will have to consider the risk and potential severity of financial loss or physical damage.

An example would be:-
*The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or alteration of a staff internal telephone list.*

Please note that any notifiable breach must be reported to the ICO within 72 hours of the business becoming aware of it.

### What breach of data needs to be communicated to the data subject?

The GDPR states that the ICO should be notified if there is a risk and the data subject should be notified if there is a "high risk".

Whether a breach presents a "high risk" is a decision that the business will have to make. The GDPR states that you do not have to inform the data subject if:-

1. The data is encrypted or protected in some similar way.
2. The business has taken steps to ensure the risk has been neutralised.

A risk can be communicated collectively if it relates to a large number of data subjects e.g. a press release.

### Who is responsible for data?

Businesses that are responsible for data are known as "Data Controllers". As a hospitality business you will almost certainly be a Data Controller.

You might from time to time have a legitimate need to share data with other entities and in these circumstances it is important to identify who may be capable of utilising data, for which your business is ultimately responsible, in such a way that gives rise to a breach.

These other entities may become joint Data Controllers with your business and common examples of other entities that a hospitality business might come into contact with include:-

1. Suppliers.
2. Marketing companies.
3. Professionals such as lawyers and accountants.
4. Businesses that you outsource employee matters to such as wages and HR.

In these circumstances it is advisable to enter an agreement with other Data Controllers to ensure that they exercise the appropriate level of care with your business' data and properly identify how each party complies with their obligations.

### How do I protect personal data?

The first thing to do is to identify the data that you hold and where it is held. Thereafter you can evaluate the protections that you have in place.

A Data Protection Policy is required and this should amongst other things, cover how your business:-

1. Collects personal data.
2. Retains personal data.
3. Uses personal data.
4. Deals with a personal data breach.

Once a business has gone through the above process and devised a data protection policy, it is then imperative that steps are taken to address any vulnerabilities. Such steps can include improving IT security and provide regular staff training.

### What sort of personal data can I collect?

A business should only collect and retain personal data that is necessary for the purpose for which it is offered by the Data Subject. For example, when making a reservation a business may request Credit Card details but would have no need to ask a customer for bank account details, or National Insurance Number, as these would not be relevant.

### How long can I keep their personal data?

A business can only keep personal data for the period of time that it takes to complete the purpose for which it is being retained.

A customer might give you Credit Card details to make a purchase and so the business will have to make a judgment on whether there is any justifiable reason for such data to be held after that purpose has been fulfilled.

Businesses will need to include provisions in their Data Protection Policy that deal with the destruction of both physical and electronic data.

# What if there is a problem?


**What do I do if there is a breach?**

You should put into action the breach sections of your personal data policies. This should include:-

1. Considering whether the breach should be reported to the ICO.
2. Considering whether the breach should be reported to the Data Subject.
3. Recording the breach on an internal register.
4. Mitigating the breach where possible. For example retrieving lost documents, notifying the Data Subject etc.
5. Fixing whatever went wrong.
6. Implementing a PR strategy to deal with any negative publicity.

There are insurance products that provide some cover for businesses that suffer personal data breaches. This is something that could be of assistance.

**What will the ICO take into account?**

Once the ICO is notified of a breach it will take various matters into account before deciding on its response. These include:-

1. The sensitivity of the personal data lost, for example, medical details.
2. Whether the business notified the ICO in good time.
3. Whether steps to mitigate the breach have been successful.
4. The steps taken to prevent breaches in the first place.
5. In general, the seriousness of the sanction applied by the ICO will be dictated by how seriously the business takes its obligations.

The ICO is aware that nobody is perfect. It is likely to look favourably on businesses that have taken precautions, have put in place all the proper procedures to prevent a breach in the first place and have handled matters in an open and transparent manner after a breach has occurred.

This open and transparent approach, together with proper due diligence, will undoubtedly help a business in the court of public opinion also.

# GDPR: What next?

| BUSINESSES SHOULD | CHECK |
|---|---|
| 1. Identify the personal data they hold. | |
| 2. Identify and record how that personal data is gathered and stored. | |
| 3. Identify the purpose for which the personal data is held and, if necessary, get consent. | |
| 4. Dispose securely of any unnecessary personal data. | |
| 5. Implement/Review/ Update their data protection policy and procedures. | |
| 6. Identify other Data Controllers and enter into appropriate agreements. | |
| 7. Review IT security arrangements and IT procedures generally. | |
| 8. Fully train staff and continue to do so on a regular basis. | |
| 9. Amend employees' contracts to cover personal data issues. | |
| 10. Notify employees and customers where, for example, CCTV is in use. | |
| 11. Periodically review all of the above. | |
| 12. Have a contingency plan (which could include insurance). | |

## Talk To An Expert

Whilst this guide sets out the basics of GDPR and compliance measures, it cannot cover all aspects of GDPR or be used as a legal defence. If in doubt, contact:

**MTB Solicitors**
88 Victoria St, Belfast BT1 3GN
Tel: 028 9032 9801

MTB

# Hospitality Ulster

HEAD OFFICE
91 University Street, Belfast BT7 1HP

**Telephone** (028) 9032 7578
**Email** enquiries@hospitalityulster.org
www.hospitalityulster.org

HospitalityUlster
@HospUlster

tourism northernireland