The General Data Protection Regulation

Data Security

Under the General Data Protection Regulation, all businesses are obligated to process personal data in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

In implementing the General Data Protection Regulation in your business you ought to consider if your current processes are sufficiently robust or what adaptations, if any, are necessary to ensure that the personal information a customer provides you with is secure. In deciding whether or not customer data is held securely you should consider if it was your data, would you be happy with how it is being held and handled?

Think of the following scenarios and whether the customer would be satisfied that their data is secure and can't be used by someone with no need to access it:

- **I leave completed application forms on the desk in my office and post them all at the end of the week**
- **I keep details of all my enquiries and plan holders' information so that I have a record in case I need it**
- **I don't use a password on my computer - I keep forgetting it and it causes a problem when a member of my staff needs to use the computer**
- **I don't trust technology - I prefer to write everything down on paper**
- **I copy all next of kin names, addresses and phone numbers into my diary and mobile phone in case I need to get in touch with them**
- **I email customer details to my other branches so all staff can access them**
- **I use a USB stick to store plan details so that I always have it with me**
- **Visitors to the business premises regularly access our back office areas to use our desks or access other areas of the business**

In each of the scenarios above there is a risk that customer data could be accessed by someone with no authority or requirement to access it. The obligation lies with you to ensure customer data is held securely and if you fail to do so there is potential for significant monetary fines from the Information Commissioner's Office - in addition to the reputational damage mishandling of customer information could cause your business.

The General Data Protection Regulation

Data Security

Your business has to determine what steps are reasonable for you in ensuring that all customer data is secure. We suggest that you should do the following as a matter of course:

- **If storing customer documentation in the office, it should be kept in a secure location where it cannot be accessed without permission, for example in a locked drawer or locked cupboard. Keys should be held securely and not left out in the office to allow anyone access.**
- **Securely destroy all paperwork once it is no longer required, for example shred all paperwork onsite.**
- **Password protect all documents containing customer data. The password should be sufficiently complex, updated periodically and only shared with those who require access to that information.**
- **Electronic data is more secure than hard copies and the risk of accidental loss, destruction or damage is significantly lowered by the ease with which you can recover electronic data; paper is much easier to misplace or destroy by accident.**
- **Avoid copying customer data to another location - access it from its original location each time you need it, for example do not copy next of kin details or funeral arrangements to your mobile telephone or personal diary but use their details directly from the database if you need to contact them. There is an additional risk here as if the customer wishes to exercise their right to be forgotten then you may struggle to account for all instances where the customer's details are held.**
- **Encrypt any emails containing customer data. Before sending you should consider if sharing the customer data is necessary or whether it could be anonymised or removed.**
- **Portable hardware such as USB sticks, portable storage devices, tablets, mobile phones etc. should always be password protected and stored securely when not in use.**
- **You must consider who has access to the areas in which you have customer information available; doctors, 3rd party company representatives etc. do not require access to all of your customer information, therefore access should be limited to only those who require the information. Secure doors such as keypad entry or lockable doors will stop unwanted visitors entering restricted areas of your business.**

In terms of data security, this includes considering who requires access to any personal data you hold. Unless you can satisfy yourself that each member of staff requires access to the personal data of any individual customer, then they should not be able to access any information that would allow them to identify who the customer is.

The General Data Protection Regulation

Data Security

Breach Notification

A data breach is where someone without requirement or authority has accessed customer's personal data. Examples of data breaches may include:

- Posting paperwork that includes personal details to an incorrect address
- Leaving password protected computers unlocked and a 3rd party viewing the customer information on the screen
- Customer paperwork being left on the desk in a locked office overnight, however the company cleaner has access to clean the office
- Whilst detailing funeral arrangements in a paper diary, the bereaved family can see details of all customers you have met with that day

You should review any current internal data breach notification processes you have in line with the General Data Protection Regulation, otherwise you must create one.

Under the General Data Protection Regulation you must inform affected customers of the breach without undue delay where there is a high risk of customer detriment. One of the main reasons for informing customers is to help them take steps to protect themselves from the effects of a breach e.g. identity fraud.

You must also inform the Information Commissioner's Office of any data breach that may cause emotional distress, and physical and material damage to a customer within 72 hours of your business becoming aware of the breach.

An example of when you would need to notify the Information Commissioner's Office of a breach and the customer of a breach would be the loss of a paper diary containing customer details, the data of which may be passed onto 3rd parties to misuse. On the other hand, you would not normally need to notify the Information Commissioner's Office, for example, about the loss of a staff telephone list.

If you require further information on implementing the General Data Protection Regulation in your business, we recommend the Information Commissioner's Office (ICO) website or helpline for small businesses (0303 123 1113- Option 4)