



Customer Guide to **GDPR**

So data protection is extending into business world, this document sets out to inform Red Flag Alert Customers and guide you to make a few basic decisions for your business.

These new rules also contain a lot of detail about protecting data and companies obligations to report breaches and loss of data.

1. Managing Data

First thing to do, you need to categorise your data, and the processes you use to manage the data. Importantly you also need to find all the data held within your business, and begin answering a few questions to determine what your auditable decision trail is...

Here are the 3 I recommend you answer first

1. Do you know where all your data is?
2. Is all your data clean and up to date?
3. Have you updated employee policies to be GDPR compliant?

So your first duty under GDPR is you must know where your data is, this must be up to date and clean data, and relevant to your day to day business. Importantly this is where you need to start making decisions that transfer into employee policies and business planning. Cyber Security goes hand in hand with GDPR so you need hr policies dealing with breach protection, destruction of redundant media i.e. laptops, mobile phones, memory sticks etc...

On the point of security you should now be thinking about levels of access to data, which employees have the right to amend data, and how you secure important data as 90% of all breaches you are likely to be fined for will be a consequence of an Employee failing to protect the data i.e. password breach, loss of equipment with data, or targeted hacking via social engineering of an employee.

2. Business or Personal Data

So practically lets split Business Data from personal data. Any corporate business registered at companies house is Business Data; however if the business is not registered and is non limited then this is now Personal Data, a small further complication is the term Micro Business, I would categorise these as possibly limited, with one or two people involved, and possibly using residential addresses.


Personal data is now more widely categorised as:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.' (Article 4)

So for the majority of businesses this will mean mobile or direct dial phone numbers, name@ email addresses, postal addresses. But importantly this should not stop you from selecting an individual or maintaining an individual's data within your business.

What you have to do is deal with why it is relevant to you, and then look at what is a fair and reasonable use of the data using legitimate interest, to be clear the ICO have stated they would prefer you have a legitimate interest use for the data over all other permissions.

"An important note to make here is that electronic communications have a distinct set of data protection regulations (PECR) which means specific consent must be obtained for marketing using electronic communications specifically email and text message or automated phone calls"



So whilst legitimate interest is useful, it is only appropriate where you intend to use direct mail or telephone calls and these must be screened against both TPS and CTPS registers. I would suggest that your business first addresses the relevancy of this data in its day to day environment i.e. its use, and terms of use, and how you audit its use. You must also be able to answer any request to be forgotten by an individual.

3. Balancing legitimate interests

It is important that you balance your requirements to use personal data, versus the rights of the individual, but in most cases you will be targeting a business, using profiling to determine why you want to contact a specific target business, and not necessarily an individual, although from time to time your marketing may specify a certain identifying piece of personal data i.e. job title.

You will need to ensure any data used is relevant to you, I would also suggest you decide what is reasonable and fair use of the data, and therefore have an end date for expected use of the data, in preparing each set of data used in this way, you are setting good business practice, and creating an auditable trail for any future investigation of your business.

4. Auditable Data

So Red Flag Alert will keep your data clean and relevant, the final piece of the puzzle is to create policies around how and why you choose to use a dataset or profile. By taking these steps you are creating an auditable trail. All staff members should be trained to understand GDPR, and the companies Audit Procedures.

Your business will also need policies on how to handle “right to erasure” requests and “subject access requests” where you must provide individuals with the specific data requested that your business holds on them.

1. Why you selected the data
2. Legitimate Interest reason for using the data
3. How you will use the data, DM, Telesales, or PECR
4. How long will you use the data i.e. length of campaign
5. Remove any data from systems that produce marketing that is not in use
6. Maintain a register of do not contact requests

If you would like more information, please get in touch.
redflagalert.com or **0344 412 6699**