

GDPR at a Glance by RGA

Are you adjusting to a new data environment

Do you ask your customers for permission before you use their data? Do you go a step further and tell them what it will be used for? If the answer to either – or both – of these questions is no, you could be in trouble if you don't start changing your ways before the GDPR deadline.

As soon as possible you need to make a list. And, if your company is anything like some of the ones I have worked with over the years, it is likely to become a very long one. This list is going to have to include – Every Single Database. AND YES, that includes, every spreadsheet, .csv file, Filemaker Pro, Access, Salesforce file, etc., on every laptop, computer and server that contains “personal” data, and, don't forget to “tag” the origins of the data! GDPR compliance will require all your databases syncing. **Where are the areas of biggest risk?** If you don't know, you'll need to find out. A data inventory exercise is daunting but there's a wealth of information out there on how to do it.

Need to Know:

- Where the data is stored
- What data it contains (i.e. fields)
- How many records
- When it was created
- When it was last used
- Where it was sourced
- What is it used for

HELP IS AVAILABLE

RGA specialise in the meetings & hospitality industry. We have worked with organisations of all sizes, both in the UK and internationally, to support a wide range of data cleansing and enhancement requirements. We can quickly telephone contacts on your database to:

- Capture clear consent for your marketing communications
- Establish a robust audit trail around consent for compliance purposes
- Verify and validate existing email addresses and obtain opt-in consent
- Append new opted-in email addresses to contacts in your database
- Build new opted-in lists to match your specifications

In addition, we can carry out a full refresh of your data, validating and enhancing existing records (job title, role, responsibility, product interest) and profiling contacts to capture valuable insight to increase the relevance of future communications.

Marketing only to those individuals who are receptive to your offer will make your marketing communications more effective, increase conversion rates and ROI, and reduce customer churn. It is an opportunity to reactivate lapsed accounts, build a deeper understanding of customer interests and generate new business from your existing data assets.

GDPR at a Glance - Email marketing

The Privacy and Electronic Communications Regulations (PECR)

It is widely anticipated that PECR will be replaced by new e-Privacy Regulations in May 2018

The only difference between B2C and B2B marketers now is in connection with email and text marketing to employees of corporate organisations. When dealing with sole traders or partnerships, the rules governing B2C marketing will apply to B2B marketers so the general position for email and sms will be that you will need opt-in consent. For telephone and direct mail, you need to offer an opt-out. The present understanding is that if you have had an existing email exchange with a prospect or customer this will be considered consent.

When dealing with employees of corporates, that is limited companies, LLPs, partnerships in Scotland and government departments, the rules for telephone and direct mail are the same, opt-out. However, when emailing or texting, you do not need the prior consent/opt-in from the individual. You can therefore send them a marketing email/text as long as you provide an easy way to opt-out of future communications from you.

For any B2B marketing communications, regardless of channel, the content must be about products and/or services that are relevant to the recipients' job role.

- Clear and plain language must be used
- Consent must be freely given, informed, specific and unambiguous
- The individual must agree by a clear affirmative action
- Pre-ticked boxes or silence will not equal consent
- The right to object to marketing must be made clear

RGA Databases: We are following GDPR guidelines – RGA's Research Procedure Document Opt In /Opt Out

<http://www.privacy-regulation.eu/en/recital-47-GDPR.htm> (see excerpt below)

- Each contact on our database is telephoned (approximately every 6 months) to determine their interest and relevance in receiving direct marketing information from MiCE venues and services
- Our research team speak directly to the named individual, colleague or a company representative (identified on our internal database) and explain the information gathered will only be provided to RGA's network of Meeting and Event venues / suppliers.
- Our databases include the type of contact who provided the information and preferred delivery (post, email, telephone) for direct marketing communications
- Regular communication with our contacts enable us to immediately address changes
- The date we made contact with the individual is logged on our internal database
- RGA data is provided on a 12-month usage licence. Together with, a data refresh facility, so, amendments can be made to the data annually
- Telephone numbers and company addresses included in our databases are those registered in the public domain
- RGA store and transport data in compliance with GDPR and Cyber Essentials guidelines.

RGA data is available for up to 12 months multi-channel use (single site/single brand), as a client prospecting tool for MiCE products and services. OPT-IN contacts collected during that time may remain on your system. However, in compliance with GDPR these contacts should be regularly updated. As we are updating our data circa 6 months, our [refresh facility](#) can help meet this requirement. Plus, providing you with amendments and additions to the data at regular intervals.

GDPR may be onerous but it's not all bad news. In fact, it presents an opportunity to transform your relationship with your clients. It just calls for a new approach and a new way of thinking. In the longer term the GDPR presents a great opportunity to get your data in shape and communicate more closely, strengthening trust and engagement with clients.

Gwyneth Gibbons, Managing Director – 01993 822303

Recital 47

EU GDPR

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.

The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

This page can also be addressed <http://www.privacy-regulation.eu/en/r47.htm>.