

Air Marketing Group Limited
GDPR Readiness Statement for our clients

1st May 2018

At Air Marketing Group, we are committed to GDPR readiness.

As our client or potential client, we aim to give you confidence in our operation and provide guidance for yours. When it comes to GDPR, there is already enough confusion, so we've decided to use plain English to explain how we have got ourselves ready. This document is not going to confuse the matter, only make it easier to understand.

GDPR is an important change in the way that data is governed, and we welcome its guidelines when it comes into effect on 25th May 2018. Although there is much that is still to be defined in how GDPR will really work in businesses, we have taken a common-sense approach to ensuring we are ready, both inwardly and when it comes to the data we process on our clients' behalf (your data).

We have been working with external experts for several months to ensure that we are as ready as we can be, so you can rest assured that you're using a supplier you can trust with your data. All our work on GDPR readiness has been based directly on ICO guidelines, information and examples and you can read more here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>.

The points set out below reflect the current state of the GDPR and the UK Data Privacy Bill. These are still not live and therefore there could be some changes particularly when there is case law on any disputed articles.

We have gone ahead so as to be ready and will make adjustments during reviews on a regular basis as new information comes to light.

Legitimate Interest vs. Consent (These are 2 of the 6 ways you can lawfully process data, that you need to worry about)

The ICO state that, with GDPR in place,

"You must have a valid lawful basis in order to process personal data."

And,

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.

There is much confusion around GDPR and one of the most common misconceptions is that GDPR will restrict us from contacting potential customers unless they have 'opted in' (given consent). It is true that consent is one of the 6 valid reasons for processing data. However, whilst gaining consent

1st May 2018

is a great way to ensure compliancy, businesses may also process data and contact data subjects, which in our case are decision makers at businesses, with legitimate interest.

The ICO provides the exact definition of legitimate interest as follows:

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

N.B As our client, you are the data controller and we are the third party (data processor).

In Layman's terms, this simply means that there must be a clear and documented, legitimate interest for processing that data. If running your business and trying to grow your business is not a legitimate interest in life, then what is?

With each of our client's campaigns, we will simply need to document a 'legitimate interest statement', outlining the reasons we need to process the data to do our job. This will be something that both you and Air will sign off and authorise. This will outline who we are targeting, why we have chosen the data subjects we plan to target, what our objectives are and what the qualifying criteria has been to select these. Documenting our purpose, processes and how we intend on using data is vital to GDPR readiness.

For our existing clients, you'll know that we have always done this anyway in your Campaign strategy form that was completed as part of the setup of your campaign, prior to launch. We will simply be amending the wording on this to ensure that nothing is missed.

So, in short – Do we need consent to market and sell to people.... No, we don't.

Data supply within your campaign

We will continue to use data that is licensed to you, our clients, from third party data suppliers. We have obtained a GDPR readiness statement from each of our data supplier partners and they have been vetted to ensure that we have documented, sufficient evidence that the data has been obtained and maintained in line with relevant guidelines.

Data obtained from a third-party supplier will be licensed to you, our client, rather than to us. You will hold the data as the 'data controller' and we will act as a 'data processor'.

Together, we have a shared responsibility to stay within GDPR guidelines. In Layman's terms, this means the following things (below each point we have explained what we're doing/have done):

We must:

1. **Transfer data to and from each other in a secure manner;**
We will be providing a secure data transfer platform to any clients where this is not already in place.
2. **Store data in a safe manner/ environment;**
We use Microsoft products such as SharePoint to store documents and files. If we hold any of your data, it will be saved in a restricted folder, available only to those who are authorised

to work on your campaign. Furthermore, our CRM (We call it CMA) is encrypted and protected with an SSL certificate, making it difficult to access unless you're meant to be accessing it. It is hosted on a secure, virtual server which is backed up each day. Only authorised personnel can access data on your campaign in our CRM. It is password protected and all transactions have an audit log (meaning we can see who did what). We will not allow multiple versions of data to be saved or used, for version control and we do not store or save your data anywhere else.

3. Maintain the accuracy of data;

This means we must update data as we use it (we do this now, already) and we must not knowingly store or use inaccurate or old data.

4. Not store data unnecessarily;

In line with the above point on maintenance, we must look to reduce risk by storing and holding onto only data that we genuinely have a need to. In simple terms, rather than holding your data on our system for life, your data lists will only be held by us for 6 months (this includes call recordings from your campaign) after it's used, unless it is data that we have a legitimate interest to store for longer (i.e. a prospect might ask us to call back in a year's time). Don't worry, we will make sure you have a copy of your data before we delete it from our system.

5. Manage data access;

We have implemented access controls so that only those in our business who are involved in your campaign can access the data that you own. Put simply...who has access? Do they need access to do their job? If the answer is no, then they shouldn't have access.

6. Allow data subjects (your contacts) the 'Right to be forgotten' and have a process to fulfil this;

Everyone now has the right to be forgotten, which simply means they want their data deleted forever. We must be able to evidence that this has been actioned and we will be implementing a process whereby we flag these data subjects in your data and they will immediately be inaccessible to our team. We will also provide reports to you to prompt you to do the same with any data you hold on that person, unless any other legal framework requires that personal data be held. Examples are Anti Money Laundering, HMRC records, etc.

7. Have a process for Data subject access requests;

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed,
- access to their personal data;
- and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Again, in simple terms, this means that we must provide a data subject a copy of all the data we hold on them (in B2B this will mostly only be name and email) within one month. Again, we are implementing a process to be able to fulfil this. We must also notify you directly as the request, in theory is made to you (as you are the data controller). You will need to be able to action this. As with the right to be forgotten any individual must be positively identified as the person making the request.

8. Ensure that you are complying when we provide your data to you;

This includes call recordings, your own data that we've updated, booking forms and much more.

All of the GDPR guidelines apply to both us and you, so please don't sit back and think that we've got you covered; we haven't.

Anything that we're doing, you should be looking to implement in your operation too, subject to your own processes and systems. **If you would like help, talk to us** and we can put you in touch with our external consultants who have helped us prepare. We cannot be liable for what you do with data in your business, we can only help educate you.

9. Use the TPS & CTPS to wash all data before it is used and on an ongoing basis;

Already in existence the CTPS and TPS allow people to register a phone number as 'not wanting to receive sale calls'. Data must not be processed and certainly cannot be called without this happening first. There is a cost to running data through the CTPS/TPS and we can do this for you via the ICO. Our third-party data suppliers all provide data that has already been washed.

10. Only use compliant suppliers and demonstrate good supplier control;

We have gathered GDPR information from all suppliers who could potentially have access to your data. This includes our IT support company, our system platform (SharePoint) our Virtual storage supplier, our phone system supplier (call recordings), our email sending platform and email supplier, our CRM software development company and our data suppliers. Please ask if you would like to access any of this information.

11. Train and educate our employees;

Awareness is key so all data processors (staff who use your data) must have a working knowledge of the GDPR and how it impacts their role and responsibilities. We are currently training our entire team, ready for May 25th.

12. Document processes;

We will be updating all documentation to evidence the changes we have made to be GDPR ready. All our systems and records will be updated, as well as all relevant policies (e.g. data retention policy, data management policy). We are also ensuring that our operational policies clearly outline how we process and use data in our campaigns. We recommend you review your documentation too.

Can you supply your own data for your campaign?

Yes, you can continue to do this, if you wish. However, before agreeing to process your data and call from it, we must implement a more stringent process to ensure that we will be compliant in doing so. Therefore, we may ask you to provide a written statement, giving detail on where the data has originated from, the accuracy of the data, and what legitimate interest we have that allows us to process the data. This is to cover **us both** and ensure that we are all compliant and protected.

For your records, examples of data we hold for you/on you are:

1. **Your contact/data lists** – Personal names and emails of your customers or potential customers
2. **Your details** – As our client, we hold your contact and personal information.
3. **Call recordings** – We record our phone calls meaning every call recording allows us to identify an individual person.

And finally... An exciting announcement!

With GDPR coming into place and the amount of change that has been necessary, we have unearthed a few system restrictions with our CMA which meant we had to find work arounds to be ready.

Whilst we have managed to achieve that, this has led us to the decision that it would be a great time to rebuild a new, industry leading CRM platform. We are excited about this as it is an opportunity for us to deliver more value to you, our clients. We will be able to offer even more transparent reporting, more live time information on what's happening on your campaign, more dynamic analysis and feedback platforms for your campaign and better user experience for you. It will also be a platform that increases productivity and communication between you (our client) and your team at Air, making it easier to achieve and measure success together. And, of course, it will be built with the GDPR in mind, making our systems fit for purpose.

Our new CRM (we've not named it yet), will be in place by the end of 2018 and is another investment in ensuring that Air is and remains 1) ahead of our competition, and 2) your chosen supplier for all your business development and telemarketing needs.

If you have any questions relating to your campaign and the GDPR, please contact us and ask.

And if you need help preparing your business for GDPR readiness, please let us know and we will happily refer you to our advising consultants.