



data|hq

# DATA COMPLIANCE & BEST PRACTICE



DataHQ



DataHQ



data-hq-ltd

## Understanding Our Regulation Strategy

At Data HQ we're constantly reviewing our policies to ensure everything we do is compliant with industry regulations and best practice. Here we review the varying regulations and best practice we adopt:

### REGULATION - DPA, PECR and GDPR compliance

Currently our B2B data is compliant with the Data Protection Act (DPA) and the Privacy and Electronic Communications Regulations (PECR). And, as far as we understand, it will be compliant with GDPR when it comes into effect in May 2018.

At the time of writing, the Information Commissioner's Office (ICO) are still unclear about their implementation of GDPR so neither Data HQ nor any other list supplier can guarantee compliance until the ICO have confirmed it themselves. We have a good understanding of the current guidelines and if our understanding is correct, our B2B data will be compliant with GDPR.

The data that we provide of sole traders and partnerships on our B2B universe file is all opted-in.

### Registration with the ICO

Data HQ is authorised through the ICO to process data for direct marketing purposes. As an independent authority, the ICO works in the public interest to protect data privacy and to uphold information rights in the UK.

If you are handling personal data of any description (including marketing lists) you should be registered with the ICO. Registration is quick and easy and can be done using this link <https://ico.org.uk/for-organisations/register/>

Personal information / data is defined 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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

## DMA and the DMA code of conduct

Data HQ have been members of the Direct Marketing Association (DMA) since 2001. As long standing members we adhere to and promote the DMA Code of Conduct as follows:

### List Rental - Respecting Privacy

Some people find it irritating and distasteful that their contact information is passed on and shared between organisations. You will get complaints from time to time it is the nature of the beast. You must take action when someone complains, apologise, say that you purchased the data in good faith, make sure you remove their record from all of your systems and preferably add the email address/telephone number to your global suppression file of opt-outs.

### List rental - Being Honest and Fair

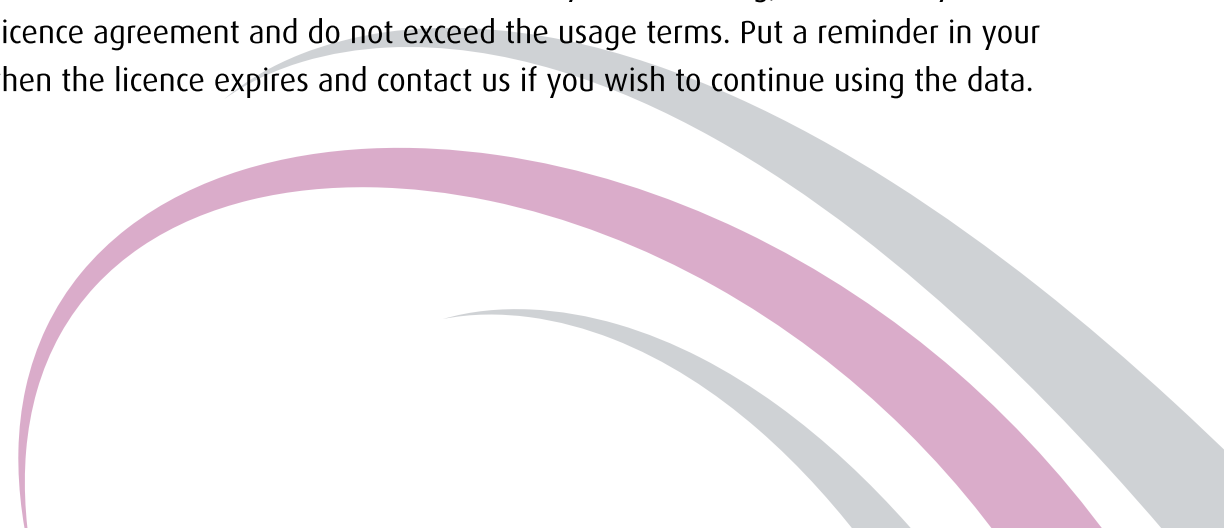
You do not need to hide any details from a complainant, tell them what how why and when, reassure the complainant it won't happen again with yourselves and pass on our details to them, we follow a strict process to handle any complaints in a quick and professional manner. Data HQ contact details for you to pass on with regards to questions or being removed from a list are: [datacompliance@datahq.co.uk](mailto:datacompliance@datahq.co.uk) 01245 807470.

### List Rental - Being Diligent with Data

Be careful with whom you share this information with and make sure you and they understand the implications of losing control of the data. It is very easy for insecure IT systems to be breached or for one person to email a file to another person without your knowledge. Once the data is in your possession the best way to transfer it is via a secure file-sharing platform such as dropbox with password protection.

### List Rental - Taking Responsibility

You are responsible and accountable for the use of the list you are renting, make sure you understand the licence agreement and do not exceed the usage terms. Put a reminder in your calendar as to when the licence expires and contact us if you wish to continue using the data.



## CTPS and TPS

The Corporate Telephone Preference Service (CTPS) is the central opt out register whereby corporate subscribers can register their wish not to receive unsolicited sales and marketing telephone calls to either all their organisation's telephone numbers, or to certain numbers. It is a legal requirement that companies do not make such calls to numbers registered on the CTPS.

The Telephone Preference Service (TPS ) is a central opt out register whereby individuals can register their wish not to receive unsolicited sales and marketing telephone calls. It is a legal requirement that companies do not make such calls to numbers registered on the TPS. The original legislation was introduced in May 1999. It has subsequently been updated and now the relevant legislation is the Privacy and Electronic (EC Directive) Regulations 2003 PECR.

All Data HQ B2B data is updated monthly and suppressed against CTPS and TPS, therefore no numbers we supply should be on CTPS or TPS.

## Best Practice

### Email Marketing Platforms

Not all email-marketing platforms allow you to use rented marketing lists whether they're opted in or not. You should always check the T&C's of your provider. If you find that your provider will not allow you to use a rented list please contact us. Data HQ can manage your email broadcasting for you and provide automated and lead nurturing programs to help with your campaigns.

### Updates and Maintenance of Data


Maintaining any personal data you hold is fundamental to the Data Protection Act, be it a rented list or any customer data. If you are renting a list from us for a license period longer than 3-months we recommend you have the list updated and refreshed by us every three months.

### Seeding and Tracking Use

We always track the use of the data we supply. We do this primarily as a data compliance procedure. It is fundamental to the DPA that personal information is kept up to date. Therefore, when your license to use the data expires (e.g. After 6 months or 12-months etc.) we are able to monitor its use and advise you to update the data with fresh and up to date information. It also alerts us if the data has been inadvertently passed on to another organisation without your knowledge.

### Transfer of Data

When we supply marketing data we always do this via a file-sharing platform. We will send a link to our own secure file-sharing platform; we will also send a password in a separate email so that data can be accessed. All you need to do is download the data to your PC.



## Frequently Asked Questions

As well as offering advice to our clients about how to handle their data during this era of changing regulation, we're often asked about our own processes/regulation. Here is a summary of the most frequently asked questions together with answers:

### 1. What is the source of your data?

Our B2B data is originated by ourselves (Data HQ Ltd) and by 118 Data Resource Ltd. In both cases the data is compiled and updated on a regular basis over the telephone. We have two files:

**A) Corporate Contacts** is updated daily and each contact is updated once every 3 to 4 months.

**B) B2B universe file** is updated daily by 118 Data Resource Ltd and Data HQ receive a refresh of the file monthly, each contact is updated once every 12 months by 118 Data Resource Ltd.

### 2. Is your data compliant to current industry regulations?

Yes, currently the data is compliant with the Data Protection Act (DPA) and the Privacy and Electronic Communications Regulations (PECR). And, as far as we know, it will be compliant with GDPR next year. However, the ICO are still very unclear about their own implementation of GDPR so we cannot guarantee this until the ICO have confirmed it themselves.

### 3. Is your data GDPR compliant?

As stated above, the ICO have not yet confirmed the final regulation, we have a good understanding of what we think it will be and if our understanding is correct then our B2B data will be compliant with GDPR.

Our current understanding of the proposed GDPR for B2B data is this: The use of B2B data for email or telephone is different to that of B2C data. 'Opt-in' for B2B data is not required for cold marketing unless the organisation / data subject is a Sole Trader or Partnership. Sole Traders and Partnerships

will be treated the same as consumers (personal data) and will be subject to strict 'opted-in' regulation. All of the Sole Trader/Partnership data we supply is 'opted-in' and we believe that in its current form/opted in status it will be compliant with GDPR.

There are still rules for all B2B marketing communications and the key rule is you must identify yourself as the sender and you must provide the data subject with a means to remove themselves from the list if they wish.

#### 4. We have been told your data is opted in...what does that mean?

On the B2B Universe file consent is obtained over the telephone as part of the initial call to be included on the database. Confirmation is then sent via email of the opt-in reconfirming that the named data subject is definitely opting in.

The Corporate Contacts data is collected in a different way and operated on an opt-out basis but only registered (Ltd, Plc or LLP etc) companies are included and therefore this data is compliant the current regulation and with GDPR as we understand it at the moment.

#### 5. Does B2B data only need opt out and not double opt in?

From our understanding of the current GDPR guidelines, B2B data for Sole Traders and Partnerships will be treated in the same way as B2C data and therefore, opt-in is required.

For registered businesses, then opt-out will remain the standard. However, you will have to comply with other rules to use opt-out; such as providing easy route to opt-out, the sender clearly identifies themselves and includes their registration number and contact details and the message is of a B2B nature.



## 6. Who should be considered 'responsible for the data'?

If it is your own customer records, ultimate responsibility lies with the Directors of the business and / or the Data Controller of the business. If you are collecting / holding personal data of any sort you should be registered with the Data Protection Act (DPA) as a data controller.

With regards to rented marketing lists you have joint responsibility with the organisation you are renting the list from:

- It is your responsibility to check and understand that the data being provided is collected fairly and lawfully, as best as is practical.
- The owner of the data has a responsibility to collect the data fairly and lawfully and also to maintain the data in accordance with the DPA.

## 7. How can you ensure your email system will allow you to upload/use bought-in data?

Firstly, check that your email system does allow for the use of cold or third party data. Many of the widely used systems do not permit this in their Terms and Conditions.

If your email system does not state clearly whether cold/third party data is ok to use then speak to your provider directly and seek clarification. There are a number of email platforms that do allow third party and cold data to be used. Alternatively, Data HQ can manage the broadcast for you.



## 8. Who Owns the data?

It is extremely rare that a rental license agreement will allow the IP of the data to pass from supplier to client. Data HQ only ever license data for an agreed period of time; we never sell data outright or transfer the IP from us to you.

It is similar to renting a car you can use it for an agreed period of time, once that time period has elapsed the data must be deleted from your systems and must not be used again without our authorization.

If a data subject has responded positively to your marketing and wishes to engage with you or receive further information then those particular data records are released from the terms of the license agreement and are free to use as you wish.



# data|hq

