
Negotiating the regulatory minefield

Electronic marketers have to consider the implications of using email lists as a low-cost option for reaching their target audience

Research into the readership of The Informed Executive indicates that the majority of those who draw down features from the magazine's web site are owners or managers of businesses covering the core SME and corporate range, with only a minimal number of very small traders. Given the distribution of business size amongst the SME population, that means that the typical reader is responsible for a business with 10 to 60 staff.

There is a good reason for defining that readership profile: it provides a thumbnail sketch of the organisations likely to be contemplating electronic marketing. At the lower end of the scale, marketing is likely to be part of the sales function: budgets will inevitably be limited, and email marketing could appear to be a cost effective way of reaching a target audience.

Even in the true medium-scale enterprise, the dedicated marketing team to be found there will be hard pushed to sustain a full range of marketing options. Here, too, email would be seen as a low-cost 'rapid-response' solution requiring minimal resources to maintain.

In practice, there are major pitfalls for the unwary email marketer. Unless an email campaign is crafted to breach a heightening wall of spam filters, the results are likely to be disappointing, with the case for further email marketing campaigns being rejected.

How that data has been sourced and how it can be targeted to achieve specific marketing objectives, makes all the difference between delivering a ten-fold yield on the purchase price and failing to cover the costs of the complete exercise.

The data can be licensed for single use, or for multiple use either within a year or for an agreed number of mailings. Some vendors are prepared to provide the same data for outright purchase.

Since many of the suppliers broker lists from a limited number of third parties, the same data can be found on several websites: price would then determine the choice of reseller.

Artificial obstacles to trade

Irrespective of the technical quality of a planned campaign, there is a legal and regulatory minefield to negotiate before a single email is transmitted. Use of the personal data which allows emails to be targeted and addressed has been controlled increasingly by a succession of Data Protection Acts in the United Kingdom.

Some limits on how information is collected, stored and maintained are probably reasonable. But the jury is out on whether the regime now in force is more of a burden on business than the benefits to the individuals whose 'personal' data is being accessed really justify.

If UK data protection legislation were not enough of a dampener on the marketing aspirations of the SME community, the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 – PECR for short – implement a labyrinthine directive emanating from Brussels. It ensures that the honest if unwary executive can fall foul of electronic communications regulations in one respect or another.

How data has been sourced and how it can be targeted to achieve specific marketing objectives, makes the difference between delivering a ten-fold yield on the price and failing to cover the costs.

The idea of pursuing any kind of a code of best practice which goes beyond legal minimum requirements finds little favour amongst hard-pressed entrepreneurs attempting to manage their email campaigns.

Email marketers cannot easily justify mailing to a given group of targets simply because they believe that the recipients are all recognisable businesses to whom a legitimate business proposition can be made. They have to jump through the regulatory hoops and establish whether the circumstances meet one of a narrowly defined set of exceptions.

Failing to reach greatest offenders

Conceived in part to reduce the volume of emails, PECR inevitably fails to meet their fundamental objectives of reducing the volume of unwarranted material clogging up the email networks of Europe.

Though the more recent members of the EU have brought with them a disproportionately high percentage of all the organised crime associated with electronic communications, the Russian republics and the Balkan states still account for the bulk of the scams and offensive emails that reach users inside the EU.

Our contention is that the regime instituted within the European Union cannot stamp out this abuse of the Internet and, in its wake, acts unfairly against the interests of UK executives keen to develop their operations through otherwise legitimate marketing over the Internet.

Restraint on marketing

UK enterprises are being penalised for the dishonesty at the outer fringes of the EU. Until we have a more level playing field, executives could be forgiven for not wishing to spend any more time or resources on compliance than the letter of the Data Protection Act 1998 and PECR requires. They will necessarily apply the most generous interpretation of those rules to their marketing activities so long as the restraints are in place.

Being advised or even forced into committing more resources to a marketing campaign than is absolutely necessary is unacceptable to the SME community. The executives who run those businesses are prepared to observe the laws and regulations reluctantly where they see the rules running in the face of natural justice. The idea of pursuing any kind of a code of best practice which goes beyond that legal minimum finds little favour amongst these hard-pressed entrepreneurs, however.

Every business involved in electronic marketing should be adopting good practices which improve the way in which it interacts with its customers and avoids putting hard won business reputations at risk with badly managed email campaigns.



Are directives from Brussels the best way to regulate **electronic marketing** campaigns in the UK?

If UK data protection legislation were not enough of a dampener on the marketing aspirations of the SME community, the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 – PECR for short - implement a labyrinthine directive emanating from Brussels. It ensures that the honest if unwary executive can fall foul of electronic communications regulations in one respect or another.

Executives should assure themselves that the owners of email addresses have given permission for that information to be passed on. Whether you acquire the list yourself or use the services of a specialist list broker, check that the records have been collected in line with PECR and UK Data Protection law.

Factors for email success

What are the factors which can determine the success of an email campaign? The focus of any campaign should be on getting the right message to the right person at the right time.

The strictures on the acquisition and management of data which precede this invaluable information would appear to make it very difficult, however, for SMEs in the real world simply to get on with their job of communicating with potential customers.

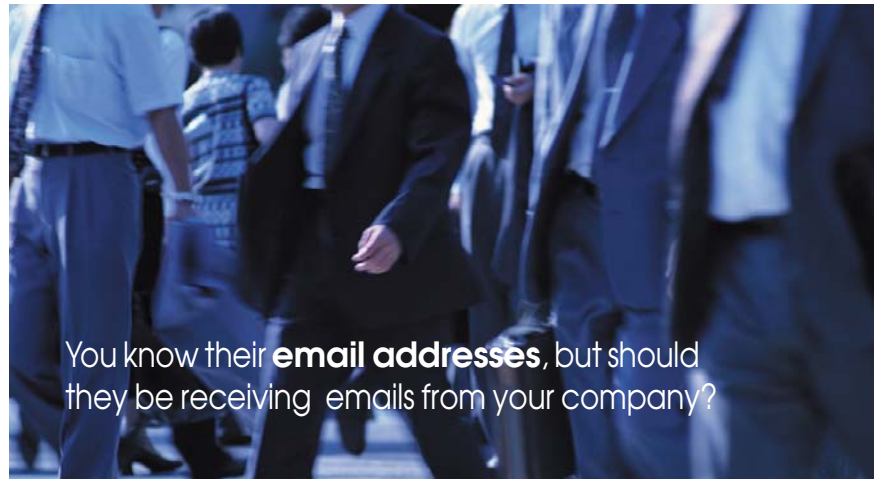
Surely smaller businesses cannot reasonably spare the same level of commitment when marketing a software product costing a few tens of pounds to 30,000 target businesses? SMEs operate on a different plane; purchasing or renting information through a list broker or buying directly from a list owner.

That is a practice which the legal purists argue is fraught with dangers, even when only business email addresses are involved. In theory at least, executives must assure themselves that the owners of these email addresses have given permission for that information to be *passed on* rather than used by the person to whom permission was given for the data to be collected and stored.

Whether you acquire the list yourself or use the services of a specialist list broker, you should check that the records have been collected in line with PECR and UK Data Protection law. To be safe, the user should secure a warranty from the provider that the data is fit for purpose and has the relevant permissions.

Little chance of warranties

From conversations with a cross section of the data community while this study was being prepared, it would appear that none had been asked for such an assurance by clients: almost universally, these companies would have been reluctant to provide one.



What confuses many executives in smaller companies is that how businesses even within the same industry have to be treated depends on their precise legal structure. There are, for example, rules about emailing business marketing materials to sole traders and partners: those constraints are quite separate from the data protection laws.

Since those formats are adopted by many start-up enterprises, the opportunities for reaching out to those businesses with products and services at a crucial time in their development are therefore tightly circumscribed by the regulations.

These segments of the business marketplace are ripe for approaches from vendors of specialist software products and office supplies, for example, phoning round such operations from the local Yellow Pages and asking for email addresses is not sufficient, it appears, even if the email addresses are given freely.

Most professional practices such as solicitors, accountants and architects operate as conventional partnerships; a construction which defines them as private individuals for emailing, even though it is for a transparently legitimate business purpose.

The argument is that what you can do with the information received during data gathering depends on the permission that has been elicited. If you make the recipient aware of the kind of material they will receive, and then provide an opportunity to unsubscribe on every piece of material mailed, there should be no problems. As long as you are completely up front at the outset, then you have covered yourself.

One way of ensuring that the data you are using is 'clean' – to the extent that the subject has given permission for it to be used – is the double opt-in process.

The email marketing regime instituted within the European Union acts unfairly against the interests of UK executives keen to develop their operations through otherwise legitimate marketing over the Internet.

“The way we collect data gives the people contacted the chance to opt out but we must presume they are aware that their details will be passed on to businesses who will then market a broad basket of goods and services to them. If we explained in greater detail very few people would be prepared to provide data.”

A person who has apparently given consent to be added to a mailing list is sent a further request to confirm that approval. In theory, it gives the data owner added confidence that valid authority has been provided to hold and then use that information in the context spelt out in the email exchange.

Double opt-in, it is argued, should not create additional work for the business securing the data as the process of sending out the confirmation request can be fully automated.

In practice, seeking that assurance is practicable when the marketing team is collating data sourced in response to a newspaper or major online campaign, for example, but does not correspond to the way in which most smaller businesses operate.

Companies easiest to target

Recipients within limited companies pose the fewest obstacles for mailing campaigns, but there are hurdles associated with every other category of recipient. Assume for the moment that a list of sole traders and partnerships has been drawn up correctly, and that permission has been given for an email to be sent.

From the regulatory viewpoint, it appears that subsequent mailings should only be to promote products or services of a similar type – and with relevance to the business.

Having secured the agreement of a sole trader to receive details of an accountancy package, it would be questionable whether the same sales operation - which also handles desks and chairs, for example - could use the same lists to mail out information about its latest furniture offerings.

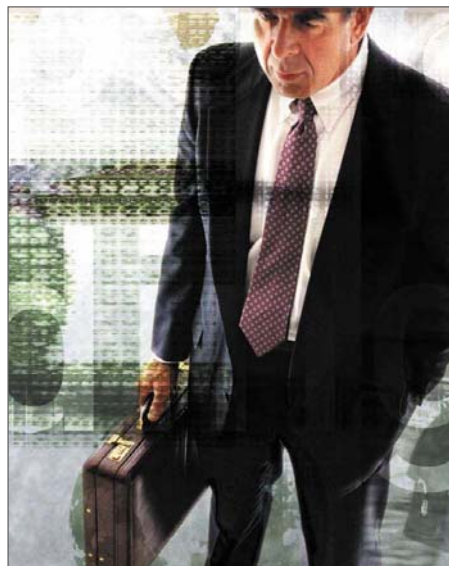
There is some difficulty in defining ‘similar products’. It is a grey area under the regulations.

SMEs have to be pragmatic

The reality of email marketing by many SMEs is determined by pragmatism rather than strict adherence to the Regulations and the Data Protection Act: in neither instance are executives seeking to abuse the spirit of the rules by inducing recipients to take part in scams, or selling their personal data to organised crime syndicates.

A list owner we interviewed in Yorkshire shares that viewpoint and operates his business in a similar vein. “The way we collect data gives the people contacted by phone the chance to opt out but we must presume they are aware – because we sell and rent out lists - that their details will be passed on to businesses who will then market a broad basket of goods and services to them.

“If we explained in greater detail that that is what would happen and sought permission for it formally, very few people would be prepared to provide data. The key is that every email sent out must provide an easy way to unsubscribe. That ensures that a recipient can be taken off any list at a moment’s notice.”



Concerns

Arguably, the list owner is not doing his job. It has to be explicit that the details would be passed on to a third party. Successful email marketing requires that there is complete transparency from the outset. While the number of people opting in would fall dramatically, those who do provide their information will be better respondents and the marketer will benefit as a result.

It would be easy to understand why executives would be reluctant to allow their name to be added to a list. If the list vendor were to sell or rent that list to perhaps a hundred customers over the space of a year, and each copy of the list were used in a dozen separate mailings, each name on the list could be the target of more than 1000 emails emanating from a single grant of permission.

And while every email letter being sent out must contain an unsubscribe facility, the withdrawal of permission to mail applies only to the copy of the list being used by that sender.

Compared with a decade ago, businesses seeking to use email as a route to market are hedged in by restrictions to an unprecedented extent.

Does e-marketing have a future?

Can emailing marketing survive as a branch of direct mail? If people trust the sender, it will continue to be a valuable channel. It is measurable and cheap and straightforward compared with a 3-month postal campaign.

Emails can be tested and tweaked and the impact on the campaign assessed instantly. If you follow the principles of best practice, your campaigns will stand out from a marketplace left muddled by the poor practices of others. More to the point, those campaigns will have higher open and conversion rates. §

Avoid the Spam Filters

ISPs employ spam protection technology to prevent unsolicited email reaching customers' inboxes. The filters rank emails against multiple criteria and if a critical limit is reached, the message is flagged as spam and then deleted automatically. A single word is not usually enough to trigger the spam cutoff, but use of multiple words such as 'Free' and 'Offer' and 'Save' can combine to reach the limit.

Maximise the click-through rate

Provide the simplest possible mechanism for readers to react. Internet links should be blue and underlined as this is what readers expect. This will increase the rate of click-throughs.

Personalise email letters

If your email records contain the title, initials and surname of the addressee, this information should be used to personalise outgoing emails. By creating a bond with the reader, a personalised opening increases the likelihood that an email will be read, and hence the possibility of a sales conversion. Figures from the US suggest that the increase can be as much as 400%. Sign off the email with your name and contact details.

Keep the message presentation consistent

Recipients soon recognise from the format of an incoming email which are the ones that they wish to read (or park for reading later). Maintaining the same typeface and layout helps enormously to keep this feeling of consistency. It would follow that newsletter formats should be cloned from each other so that the look and feel are identical – until the time comes for that style to be changed.

Experiment before a large run

It is worth running a few small samples each of perhaps 1% of the total data for a campaign to assess which one of the variants achieves the highest response rate and conversion.

Select the best day for a mailing

Experience shows that Tuesday and Wednesday are the best days for a mailing campaign. Monday is not a good day as your message may get lost in the weekend's trawl.



Ten points worth aiming for in your next email campaign



Keep the timing and frequency consistent

If you are in the habit of sending out emails at intervals, it is more logical to keep the schedule to same day of the week (or whatever interval is selected) and at the same time of day. You cannot expect readers to be poised ready for the email to land in their inbox, of course, but there is no unhelpful element of surprise. The likelihood of a newsletter or announcement from your company being deleted without being read reduces in the process.

Choose an eye-catching subject for the message

If the subject matter is not immediately obvious from the subject line, the email will be deleted or ignored completely. Use the subject line to give the reader as much information as possible about what the message contains.

Simplify the process for unsubscribing

While the UK requires that mailings should carry a method of unsubscribing, it makes sense to keep that process simple. If readers who do not want to be included in mailings cannot find the unsubscribe button, they will send emails to any address they can find and there is a real risk that the request may not be picked up. Remind anyone having the temerity to unsubscribe that they will be barred from future benefits that your organisation may offer. It may not reduce the number unsubscribing, but it will make them think twice about it.

Use the Outlook preview pane to advantage

Most PC users operate their Outlook/Outlook Express system with a preview pane showing the first few lines of the message. Ensure that the 'meat' of the message can be fitted into this valuable space as it is in view before the reader has to take any direct action to open the email fully.