Opinion Piece

Adding value to customer engagement through effective data compliance

Marie Myles

is a Strategic Client Director at Experian Marketing Services. She has a wealth of client and supplier/agency experience in delivering data- and insight-driven actions and business benefits. She blends customer-centric, data- and insight-driven techniques with pragmatic, commercial thinking. Her experience managing significant budgets and sales targets whilst client side ensures the advice and client support is delivered in a way that focuses on ROI and meeting critical client needs.

Marie Myles

Received (in revised form): 15th June 2015

Abstract

Permission to market is a vital resource for companies and one they need to nurture. This article considers some of the methods that marketers must use as a result of legislation and others that they should use in order to optimize their permission rates and reduce unsubscribe levels.

Journal of Direct, Data and Digital Marketing Practice (2015) **17,** 8–13. doi:10.1057/dddmp.2015.37

Keywords: permission marketing, data protection, direct marketing

Five core principles

The concept of permission marketing was first championed by Godin [1] back in 1999. The principles he outlined still hold true today, maybe even more so, given the growing number of ways that brands interact with their customers. At the heart of permission marketing lies robust personal and preference data management. I believe that there are five core principles that form the basis of best practice permission-based marketing:

1. Operate above minimum legal requirements and ensure your privacy policy is updated and clear;
2. Manage effective data capture and management processes;
3. Make your privacy policy visible to customers — shout about what you are, and aren't, going to do with their data to build confidence and trust with your customers;
4. Manage their permissions and your own Privacy Policy, not just at the point of sign-up, but throughout the relationship;
5. Build relevant communications (hopefully two-way) to maintain permission levels and to grow your customer base and hit business targets.

Understand the rules

So how do you go about doing this in the increasingly complex world of marketing and communications? What skills, knowledge, tools and techniques do you need for success? Before looking at the five steps to effective data compliance, we need to consider some customer and market behaviours and facts. Anyone managing personal data should be very familiar with both the 1998 Data Protection Act (DPA) and the 2003 Privacy and Electronic Communications (EC Directive) Regulations (PECR) — both are summarized on the Information Commissioner's Office website (https://ico.org.uk/for-organisations/guide-to-data-protection/).

Marie Myles
Experian Marketing Services,
6th Floor, Cardinal Place, 80 Victoria Street, London, SW1E 5JL UK
Tel: +44 (0)7854 228210

'Cookies Directive'

In addition, an amendment to PECR came into force on 25 May 2011. This particular directive required UK websites to obtain consent from their visitors in order to store and retrieve information from their computers, that is browser settings and consent regarding the use of cookies. It also requires websites to make it clear how that data is going to be used. All websites that use customer online behavioural data for targeting of content or advertising need to comply.

PII and processing

The regulation specifically relates to the processing of personal data captured in electronic and non-electronic formats. Two important definitions have implications for marketers:

- Personal data: This is defined as any information about an individual that can be used to identify that individual (even if another, non-personal piece of information is used in order to make the identification). The key phrase is Personal Identifiable Information (PII).
- Processing: This covers the use, storage, collection, deletion, re-organisation, retrieval or consultation of any relevant data. Note that this has to be relevant and genuine for the purposes of running the business and needs to be fair and lawful.

Understand customer attitudes

For people like us who collect, manage and interpret customer data, increasing concerns about the privacy of PII expressed by consumers are a challenge. Trends in the opt-out rate from the Electoral Roll and rising Telephone Preference Service and Mailing Preference Service registration numbers are barometers of customer unease. Concerns about organisations sharing their personal information with other bodies topped the ICO Annual Tracker Study in 2013 at 37 per cent, while 29 per cent were concerned about companies keeping their information secure — well ahead of the 13 per cent worried by fraud or identity theft .[2]

Trust in social media

Data sharing has become more complex in the digital world, particularly with the development of Web 2.0 and the growth in social media applications. If you take your brand into these channels, you will also need to ensure that you understand the data protection implications of data accessed via these sites and any effects it has on your business, not only from a legal perspective, but a brand trust perspective as well.

Barriers and options

All of this means the need for best practice in data management is paramount. By adopting appropriate data management capabilities and processes and then being open and honest about them, you should be able to gain that all-important opt-in to marketing communications. But, all too often, data protection legislation is seen as a threat and barrier to customer engagement and data collection. It is perceived that privacy policies will encourage customers to opt out of — or not opt in to — future communications. As a result, we have observed marketers taking actions that try to comply by making opt-out the default message (or soft opt-in digital) or make the choices vague to keep options open. Ultimately, this is a business decision, but we believe that it is not the best approach to adopt in a world of ever-more empowered and informed customers.

Customer preference management

As the marketing ecosystem has evolved, the touchpoints an organisation has with its prospects and customers have widened. So, as you

start accessing more personal data from different sources, you need to ensure that this is reflected in your overall preference or consent management processes and systems. Today, customers can engage through the telephone, email, social networks, websites, chat rooms, face-to-face, digital TV and through their mobile devices. Organisations must now ensure that not only can a customer choose to opt in to or opt out of marketing communications, but that within a reasonable amount of time their choice is reflected appropriately across all of these channels and media.

Customer choice scenario

Let's take a scenario:

A customer may log into their account online in the evening and decide that they want to opt in to communications through one particular channel, say email. Then, in the morning on the train to work, they realise that they forgot to check that they had opted out of telephone calls. Rather than logging in again, they decide to call the customer service centre to check. They will expect that service agent to be aware of last night's amendment about email and be able to verify their current request or query.

Transparent and accessible

Recording date, times and channel of customer data updates adds to effective management of the customer experience and supports any queries from them in the future. If not real-time, then batch uploads of personal information need to be frequent enough to maintain an acceptable and accurate record of customer preferences. This can also provide data to create key performance indicators, for example, number of opted-in customers by channel over time. In terms of transparency, there is also an obligation to make it clear who you are, that the privacy policy is easy to understand, that it is written in a customer-friendly manner, that it is clear what you will and won't do with customer data, and that the policy is easily accessible.

Working with data legislation

Since the draft European Union Data Protection Regulations were proposed in 2012, marketers have faced a degree of uncertainty about the framework they will need to operate within. Regardless of the final shape of the regulations, we believe that there are five steps to effective data compliance management. They are:

Strong working relationship

Step 1 — Understand the rules and work closely with your compliance team

Make sure you get the basics right first of all. Understand data compliance rules and keep on top of developments, both in legislation and cases. Look out for examples of new ideas and best practice in other brands. Make sure you consider data compliance needs for any new channels and use your compliance team's expertise to support you.
We believe that success is probably best achieved when there is a strong working relationship between marketing and the legal and compliance team. The challenge is that compliance officers will look to enforce privacy to the very letter of the terms and obligations, though at times these are at odds with what the marketing team wants to achieve.

Constructive compromise

Our recommended approach is to work on a collaborative basis using a considered risk management approach. There are always grey areas in any type of regulation and the compliance team will know just where these are — it is from there that a constructive process of compromise and agreements should be followed. For instance, in cases where there are high opt-out rates, yet marketing wishes to communicate to that group, the team

should work together to look at options such as customer service messages to inform customers of the privacy policy off the back of relevant services messages, particularly when the policy has been changed.

Multiple touchpoints

Step 2 — Get your data capture processes right

Get it right at the beginning and benefits will accrue down the line. How good are your data capture processes? Are they compliant, that is, collecting the right data in the right way with clear privacy policy information? There are multiple touch points to collect data — are all of these covered and, if so, are they covered consistently?

Short versus long-term value

Clearly the data captured (beyond personal contact details) will vary by business and each one will also need to consider the level of preferences that they wish to manage. For instance, do you want to offer people the option to select preferred contact channels and/or tick areas of your business that are of interest to them? The risk here is that marketing people get carried away and start to ask for too many things. Not only may this be difficult to manage and maintain, but it may also deter the customer from completing the registration, particularly during a sales process. We advise that you stick to the core basics and, if required, follow up in later contacts. It may be useful to test alternatives and, as with any acquisition assessment, review the value in the longer term. If it turns out that those people who only fill in short forms turn out to be transient and low value, yet higher-value customers are happy to give more information, then you should opt for the longer forms.

Customer ambivalence

Step 3 — Data compliance audit and review of current practices

At this stage, you need to review compliance aspects at the point of data capture, both through traditional channels and digital. Of prime importance is the adherence to preferences, ie, opting out and opting in. Again, beyond the basics set out in the legislation, it is up to a business how it chooses to do this. Some argue that opt-in, even in non-digital media, is the best policy as the customer is actively consenting and, in theory, is more engaged with your brand and open to contact. Others argue that this limits the size of the contactable base too much and that setting an opt-out option is sufficient. If a customer is that concerned, they will tick that box and opt out — it could be argued that most customers are ambivalent at this stage.

Use plain English

In the digital space, the use of cookies and access to IP addresses also needs to be made clear to a customer. And it isn't just the wording that needs to be audited online — you need to confirm that your platform and the mechanism used to collect PII are secure. And, finally, the law also asks you to make your privacy policy accessible and simple to understand. So, make sure that your communication doesn't have lots of small type and legal phrases as this will disengage the customer and make them wary. Stay true to that age-old basic direct marketing principle of 'Keep it simple, stupid'. Ensure that you use plain English and be open and honest. Inform the customer about:

- What information you wish to collect and why
- How you will use it
- How you will protect it and
- What choices and control the customer will have.

Consistent preferences

Step 4 — Manage data in a single repository and preference centre

Managing customer preferences means that organisations should really organize and give access to a single view of which channels customers have opted in to and opted out of. This central preference centre must reflect the customers' opt-in/opt-out status across all channel touchpoints. If the information in the preference centre is different to that at the call centre and you outbound call the customer, they won't be best pleased if, through the web, they had opted out of telemarketing calls!

Keep data updated

Ensure that the data is updated frequently and date-stamped and that you maintain a customer preference history record. Customers' preferences and profiles also change with time, so make it simple for them to update this using whatever channel they like and ensure that data update processes are in place to maintain accurate records. Ultimately, this data is only of value if acted upon, so ensure that preference data is integral to your customer database and campaign selection and customer management plans and processes.

Unsubscribes and unopened emails

Step 5 — Managing your contact strategy

Having given a customer a reason to opt in and shown them how you will protect their information, you have made that first important step forward. The next step is to ensure that you do not damage the building of trust within the first few months. Too often, businesses over-contact customers, particularly when there are lots of products to be sold and/or there are no contact strategy controls or targeting in place. In particular, the low cost of emails has led many to a 'blasting' approach that shows little if any acknowledgement of customer preferences or needs. Given that 'unsubscribes' have to be made clear on all emails, you run the risk of customers opting out, though we would argue that serial non-openers have in fact deserted your communications and haven't bothered to tell you. Our own research has found that 60 per cent of email targets never opened an email from a brand during a 6-month period.

Centrally managed contact

Managing customer contact through a centrally managed, optimised contact strategy will prevent the customer receiving multiple emails, letters and phone calls all promoting different products in a given campaign period. The result of disconnected contact is that the customer loses trust and, at the first opportunity, opts out of every channel. Customers change their minds and opt out of channels mainly because of the organisations' poor contact management processes. As an example, a colleague purchased some clothing from a recognized online retailer about 12 months ago and, since then, they receive emails almost every week and at least one catalogue every 6 weeks from the brand. They've never responded or clicked through from the emails and hardly turned a page of the catalogue, but communications continue to come through. How engaged do you think they are with this brand?

Central buy-in

The management of a targeted and relevant customer contact strategy is built upon robust and compliant data, good analytics, the ability to convert insights into actions across media, a flexible customer database, and planning and campaign management tools. These are the base capabilities for a good customer engagement programme, but technology alone will not deliver the results. There has to be buy-in across the business to this

central customer management process, along with relevant people and processes to deliver fast and efficient programmes. Weaknesses in any aspect could lead to a slow, cumbersome and seemingly bureaucratic set of end-to-end processes – and a waste of money.

Summary

Turning compliance to your advantage

If done properly, data compliance capabilities can add value to a business. So let's not be frightened off by data compliance, but instead build a robust set of data capture and data management capabilities. Then be brave and shout about it — tell your customers and prospects what you do. Be open, truthful and honest with them. That way, you will gain trust and build stronger relationships with them. Show them that you take the matter very seriously and respect their rights. Above all, live this through targeted and relevant messages, content and contact strategies. The use of these best practice techniques should form a basis on which to drive higher customer engagement with your brand and value to your business.

Five key strategies

1. Work closely with your compliance/legal team and understand the rules;
2. Get your data capture right;
3. Be open and honest about your privacy policy and make it easy for the customer to read and understand;
4. Put the customer in charge of their preferences and manage preferences centrally;
5. Manage contact with the customer carefully in order to build trust and value.

References

1. Godin, S. (1999) *Permission Marketing; Turning Strangers into Friends and Friends into Customers*, Simon & Schuster, New York.
2. Information Commissioner's Office. 'Annual Track 2013 – Individuals', https://ico.org.uk/media/about-the-ico/documents/1042195/annual-track-2012-individuals.pdf, accessed 27 July 2015.