Contents

[2]Data protection and direct marketing – what's changed?

It's not an under-statement to say that marketers must re-boot their thinking when it comes to data protection, privacy and direct marketing.

Direct marketing isn't just about products and services. It also covers the promotion of aims, ideals and even political opinions. The application of the UKGDPR and the Privacy and Electronic Communications Regulations (PECR) are more important now given the importance of personal data in making direct marketing work.

What is changing is that direct marketing can trigger data protection and other regulatory issues for those who fail to understand and get to grips with the new digital landscape and the legal framework that regulates this activity. The consequences aren't just eye watering sanctions and fines but go much deeper – and can harm brand and corporate reputation. Training is the front-line defence to protecting business continuity for the brand owner and for marketer's data protection training must be mandatory.

From mass marketing to data minimisation

Data minimisation doesn't just extend to the quantity of personal data being processed at any given moment, it applies to all marketing activities, be focused.

Mass marketing was based on not having to do your homework – treating a large (if not millions) of customers and prospects in the same way in the hope that their behaviour would lead to the desired outcome – the purchase of a product or service. Culture, language and local market conditions were irrelevant to the advertising or TV commercial. Some TV commercials spoken in one language were often dubbed into another to save time and money in the vain hope that 'mass marketing' would achieve its desired outcome.

Then came the internet and the democratisation of having choice to shop around and compare products and services without getting exhausted in the process. This opened up the opportunities to segment potential customers and clients in a micro-way by understanding their attitudes, values, perceptions, beliefs and behaviours in ways that marketers only a decade previously could only dream of.

But this more sophisticated profiling came greater risk to the privacy of the individual and as this Paper discusses, stronger data protection, privacy and security regulations where marketing has to be seen through the lens of 'risk' and marketers are now expected to take a risk-based approach whenever thinking about processing the personal data of a customer or client. Whereas gathering vast amounts of personal data may have appeared attractive – even essential – and where technology companies promised new ways to navigate around vast 'data lakes' the direction of travel is heading in the other way. It's now a requirement that only that amount of personal data required to deliver a product or service should be processed. We've all become minimalists. It's not because personal data is a bad thing – it's because it's a resource that doesn't belong to the marketer. So we can try and control or process it, but we don't own it. At some point, we have to give it back.

Data minimisation doesn't just extend to quantity of personal data being processed at any given moment but also the access given to those involved in marketing and processing personal data of customers, clients and prospects – where access to such personal data must be on a 'need to know' basis in order to do their jobs[1].

[1] This is often referred to as the Principle of Least Privilege (POLP)

Market research and 'sugging'

Brand owners can't dress up direct marketing activities as 'research' – selling under the guise of research (known as 'sugging') if the intention is to try and sell its goods and services or to help the brand owner (or others) to contact people for marketing purposes later.

In accordance with the latest guidance published by the ICO[2], direct marketing rules don't apply if a company or organization conducts genuine market research where for example, the purpose is to make decisions for commercial or public policy or contracts with a market research organisation. However, market research companies will still need to comply with other provisions both in the UKGDPR and DPA18.[3]

The ICO guidance identifies:

"If the call or message includes any promotional material or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. The organization must say so and comply with the DPA18 and PECR19 direct marketing rules."

Falling foul of this will be a breach of the transparency principle enshrined under the UKGDPR and which permeates the entire Regulation. It could also become a breach of the Telephone Preference Service (TPS) or if a text or email has been sent without consent or is instigated by the brand owner for someone else to do so (which is a breach of PECR).

List broking

Companies and organisations can use a list-broker service if THEY comply with the UKGDPR, as well as relevant codes of conduct. What that means in practice is that your brand needs to be identified to individuals on the list when they provide consent.

To begin with, there are a large number of sources that can generate leads – phone directories, chambers of commerce directories, previous customers and clients, individuals who've shared an email address, registered on a website, subscribed to offers or news alerts, who've signed up to read a blog, downloaded an App, entered a compensation or prize draw and used a price comparison website to obtain a quote for a product or service.

[2] See https://ico.org.uk/media/for-organizations/documents/1555/direct-marketing-guidance.pdf

[3] This includes processing individually identifiable research data fairly, securely and only for research purposes.

The guidance from the ICO is that a company or organization may be able to use these sources provided that they comply with the UKGDPR data protection principles, the DPA18, PECR and of course any Codes of Conduct that would apply within the particular industry or sector.

“It must always act fairly and lawfully,” is a mantra often repeated by the ICO on this point.

What this means in practice is also spelt out in Art.14, UKGDPR that deals with the situation where personal data is processed of the customer or prospect but comes via a third party, such as a list broker, rather than directly from the individual.

A Data Privacy Notice is required to be given to the individual by the brand owner and this sets out clearly and in easy to understand language the identity and contact details of the data controller, the DPO and also third parties who are recipients or categories of recipients that will receive this personal data. It also covers any international data transfers, as well as what appropriate safeguards are in place if this was to happen to a non-adequate country as well as list of other rights and freedoms as well as how to make a complaint.

Where list brokers tend to fall down is that they are harvesting personal data in the first instance and then looking for a customer for this personal data – rather than telling the individual data subject about the identity of this brand owner (customer) at the point of collection of their personal data.

This sounds a bit like ‘chicken and egg’ but ICO guidance on this point is very clear:

“If you’re buying a ‘consented’ marketing list, the consent request must have identified you specifically. Even precisely defined categories won’t be enough to give you valid informed consent under the4 UKGDPR definition. You must keep records to demonstrate what the individual has consented to, including what they were told and when and how they consented. If you buy personal data from another organisation, you must provide people with your own transparency information detailing anything that they haven’t already been told.”

This underlines the importance of transparency, accountability and control in the hands of the data subject.

It's clear that responsibility for data protection, privacy and security rests squarely on the shoulders of the brand owner at every point in the value chain. In practical terms, the marketer must do their own due diligence and check that the list broker or other third party has acted in accordance with the higher standards of data protection, privacy and security as demanded under the UKGDPR and has obtained that data lawfully and fairly. And that means individuals understood that their personal data would be passed on for marketing purposes and that they had the necessary consent.

And where the direct marketing activity uses texts, emails or automated calls, there's a higher standard that marketers must comply with as they must have very specific consent for this type of direct marketing. Indirect consent (ie. consent given to a third party like a list broker) isn't going to be sufficient.

The ICO also warn that the 'soft opt-in' exception under PECR doesn't apply for email or text marketing for contacts on bought-in lists. In many ways, there's an 'expectation test' to satisfy – would the person receiving this direct marketing expected to have received it? It's about seeing the world through the eyes and ears of the data subject.

It maybe that buying such lists is now 'too hot to handle' and the brand owner may want to invest in building their own B2C direct marketing lists rather than spending resources on third parties to do the job for them.

Interns and students could be trained to harvest this information carefully. The starting point could be to compile lists of customers that have bought goods or services in the past, registered on the brand owner's website or made an enquiry. However, marketers can't assume that individual customers have consented to marketing and so consent will be required. It will be important to record what they were told, and when and how they consented to the use of their personal data.

And of course, brand owners should screen against a TPS list where they're thinking of calling the customer by phone, just in case the customer has joined the TPS list and calling them would be a breach that would lead to a sanction/fine.

It's also good practice for marketers to hold a suppression list as this records who doesn't want to be contacted by direct marketing given that it's an expression of the individual's right to object to the processing of their personal data for that context.

Consent on steroids

The nature of consent has been beefed up and if brand owners wans to rely on consent, then be prepared to satisfy the higher bar as a result of the UKGDPR!

Even if able to comply with these higher consent standards, the brand owner must also comply with all seven data protection principles and simply relying on consent of the data subject won't negate this requirement.[4]

For example, relying on the consent of a data subject won't legitimise collection of personal data which isn't necessary in relation to a specified purpose of processing and is fundamentally unfair.

UKGDPR

Art.6, UKGDPR provides six lawful bases for processing personal data, with consent at the top of the list. This isn't some random list of legal bases for processing personal data, although lawyers argue that each ground is equally valid given the circumstances that are the most appropriate for processing personal data.

That said, marketers will be hard pushed to find a ground that so satisfies transparency, accountability and control in the hands of the data subject. Consent in this respect is extremely useful for the brand owner but by no means is the only legal basis and there may be more appropriate grounds, such as legitimate interests, although all of them are challenging in their own way to meet.

Art.7, UKGDPR provides the conditions for valid consent and in April 2018, Article 29 Data Protection Working Party published its guidance on consent.[5]

[4] See http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[5] Ibid

Art.4(11), UKGDPR stipulates that consent of the data subject means any:

- freely given
- specific
- informed
- unambiguous indication of the data subject's wishes

by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The evidential burden isn't on the shoulders of the data subject but the data controller. This is a game changer when there's a complaint made and the brand owner has to 'prove its innocence' as the presumption will be in favour of the data subject.

Consent is central to the rules on direct marketing. Brand owners will generally need an individual's consent before they can send marketing texts, emails or faxes, make calls to a number registered with the TPS, or make any automated marketing calls under PECR.

They will also usually need consent to pass customer details on to another organisation under the first data protection principle under the UKGDPR[6]. If a brand owner can't demonstrate they've got valid consent, then continuing to process this personal data will be a breach of data protection laws.

To be valid, consent must be knowingly and freely given, clear and specific. Marketers should keep clear records of what an individual has consented to, and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint. Maintaining accurate and up-to-date records is essential.

'Freely given'

Higher standards means that the data subject must have a genuine choice over whether or not to consent to marketing.

[6] Under Art.5 (1) (a), UKGDPR personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This is known as 'lawfulness, fairness and transparency' principle.

Marketers shouldn't coerce or unduly incentivise people to give their consent or indeed penalise anyone who refuses to give their consent. It should be as easy to remove consent as it was to give it in the first place.

Where consent to marketing is a condition of subscribing to a service, the brand owner will have to demonstrate how this indicates that consent was freely given (it won't be assumed).

In its guidance, the ICO recommends that brand owners don't make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent can't be sought separately.

It's also relevant to consider whether there's a choice of other services and how fair it's to link consent to marketing with subscribing to the service. It will also be important to assess whether this approach creates an imbalance in the rights and interests between the individual and company or organization.

'Specific'

In the context of direct marketing, consent must be specific to the type of marketing communication in question (eg automated call or text message) and the brand owner sending it.

'Informed'

Data subjects must understand what they're actually consenting to.

Brand owners must make sure they clearly and prominently explain exactly what the person is agreeing to, if this isn't obvious. "Including information in a dense privacy policy or hidden in 'small print' which is hard to find, difficult to understand, or rarely read will not be enough to establish informed consent," says the ICO. This links to the fairness requirements found in the first data protection principle of the UKGDPR.

'An indication signifying agreement'

Consent must be a positive expression of choice, gone are the days of implied consent. If your boxes are still automatically checked then you WILL fall foul of the UKGDPR.

It doesn't necessarily have to be a proactive declaration of consent – for example, consent might sometimes be given by submitting an online form, if there was a clear and prominent statement that this would be taken as agreement and there was the option to opt out.

But brand owners can't assume consent from a failure to opt out unless this is part of a positive step such as signing up to a service or completing a transaction. For example, they can't assume consent from non-response to an email, as this wouldn't be a positive indication of agreement.

Privacy and Electronic Communications Regulations (PECR)

Marketers must never assume that 'consent is for life', as under the new data protection landscape, consent doesn't last forever!

The notion of consent in PECR and the proposed E-PR remains linked to the notion of consent in the UKGDPR.[7]

However, according to the ICO, the interpretation of consent in a direct marketing context with respect to electronic marketing calls or messages must satisfy an even higher standard and requires the recipient to have previously notified the brand owner that (s)he consents for the time being to such marketing communications being sent by or at the instigation of the brand owner.

"In our view, this means that consent for electronic marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific," says the ICO in its guidance.

In practical terms, this means the customer or client must notify consent to the brand owner actually sending the direct marketing communication. A company or organization must therefore be very careful when relying on indirect (third party) consent that was originally given to another company, such as a list broker (see above).

"The person must have intended for their consent to be passed on to the organisation doing the marketing" advises the ICO.

Consent for a one-off message, or consent that's clearly only intended to cover a short period of time or a particular context, won't count as ongoing consent for all future marketing messages. Consent 'for the time being' is given its literal meaning, implying consent lasts as long as

[7] Art.4(11) and Art.7, UKGDPR. Besides the amended definition in Art. 4(11), UKGDPR there's details in Art.7, UKGDPR for the conditions for consent and further explanation in Recitals 32, 33, 42, and 43, UKGDPR as to how the data controller must act to comply with the main elements of the consent requirement. Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

circumstances remain the same, and will expire if there's a significant change in those circumstances. In many respects, that's common sense.

An important point for marketers to remember is that the customer or client must specifically consent to the type of communication in question. In other words, the brand owner can't make an automated call to the customer, client or prospect unless that person has consented to receiving automated calls and the brand owner can't send a text unless they've consented to receive marketing texts. Consent to receive marketing phone calls can't be extended to cover texts or emails, and vice versa. And a general statement of consent to receive marketing might be valid for postal marketing but won't cover calls or text marketing messages.

Is implied consent dead?

Marketers can't rely on 'implied consent' as a euphemism for ignoring the need for consent, or assuming the customer or client consents in the absence of any complaint.

The ICO doesn't say it's dead but it's guidance tends to indicate that it is.

"Even implied consent must still be freely given, specific and informed, and must still involve a positive action indicating agreement (e.g. clicking on a button or subscribing to a service). The person must have understood that they were consenting, and exactly what they were consenting to, and must have had a genuine choice –if a condition of subscribing to a service is giving consent to marketing, the organisation will have to demonstrate how this indicates that consent was freely given."

On reading this, it sounds very risky to rely on implied consent. The ICO recommends that brand owners don't make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent can't be sought separately. On reading this, the presumption is clear. Marketing isn't necessary.

It's also relevant to consider whether there's a choice of other services and how fair it is to couple consent to marketing with subscribing to the service. It will also be important to assess whether this approach creates an imbalance in the rights and freedoms of the individual versus that of the brand owner.

In some other contexts, the intended use of personal data is so obvious that the act of providing the data in the first place is enough to indicate consent – e.g. providing a postal address when completing an online transaction clearly indicates consent to use that address to deliver the goods. It might be clear that the use of that personal data is a necessary part of a service or activity – e.g. if a website displays a clear banner saying that using the site will result in cookies being set, then clicking through the pages is likely to indicate implied consent to the use of those cookies, as long as sufficient information is made available to fully inform users.

However, direct marketing is highly unlikely to form an obvious or integral part of another service or activity in the same way. It will be difficult to show that a customer or client understood they were agreeing to receive marketing messages unless there was a very clear statement explaining that their action would be taken that way, and a free choice whether or not to consent.

"It is not enough for implied consent if such a statement is only provided as part of a privacy policy or notice which is hard to find, difficult to understand, lengthy, or rarely read. The customer will be unaware of what they are agreeing to, which means they are not informed and there is no valid consent" advises the ICO.

In practical terms, marketers must ensure that clear and relevant information is readily available to their customers and clients, explaining exactly what they're agreeing to and what choices they have.

In summary, implied consent in the context of direct marketing messages isn't necessarily an easier option for the marketer and is likely to require brand owners to take similar steps for explicit consent.

For example, if explicit consent can be obtained using an opt-in box, implied consent is still likely to require a prominent statement paired with an opt-out box. The ICO therefore recommends that companies and organizations use opt-in boxes in order to obtain explicit consent.

So perhaps implicit consent has just been read the last rites?