Direct Marketing & GDPR

Be compliant
and build trust

ASSIST

Contents

PURPOSE

The Information Commissioner's Office (ICO) has released a draft Code of Conduct for Direct Marketing activities[1] . This draft document is open for public consultation until it is finalised later in 2020. It is not anticipated that the final version will vary significantly from the draft as the code is based firmly on existing data protection legislation, specifically GDPR, DPA 2018 (Data Protection Act 2018) and PECR 2003 (Privacy & Electronic Communications Regulations 2003).

This document is designed to distil the core elements of the proposed Code of Conduct and provide practical advice on conducting direct marketing whilst maintaining compliance with the applicable legislation.

As awareness of what compliant marketing activity looks like increases amongst the business world (and the general population) it is imperative that you comply with PECR/GDPR not only to avoid the risk of official sanction but also to demonstrate to your customers and potential customers that you are deserving of their trust, and therefore their business. Lost opportunity is by far the biggest risk of being visibly non-compliant, and for this reason compliance is vital in building trust and loyalty amongst your customers.

Furthermore competitive advantage can be gained by putting transparent compliance at the heart of your messaging, thus differentiating yourselves from non-compliant competitors.

[1] *https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-direct-marketing-code-of-practice/*

THE LAWS

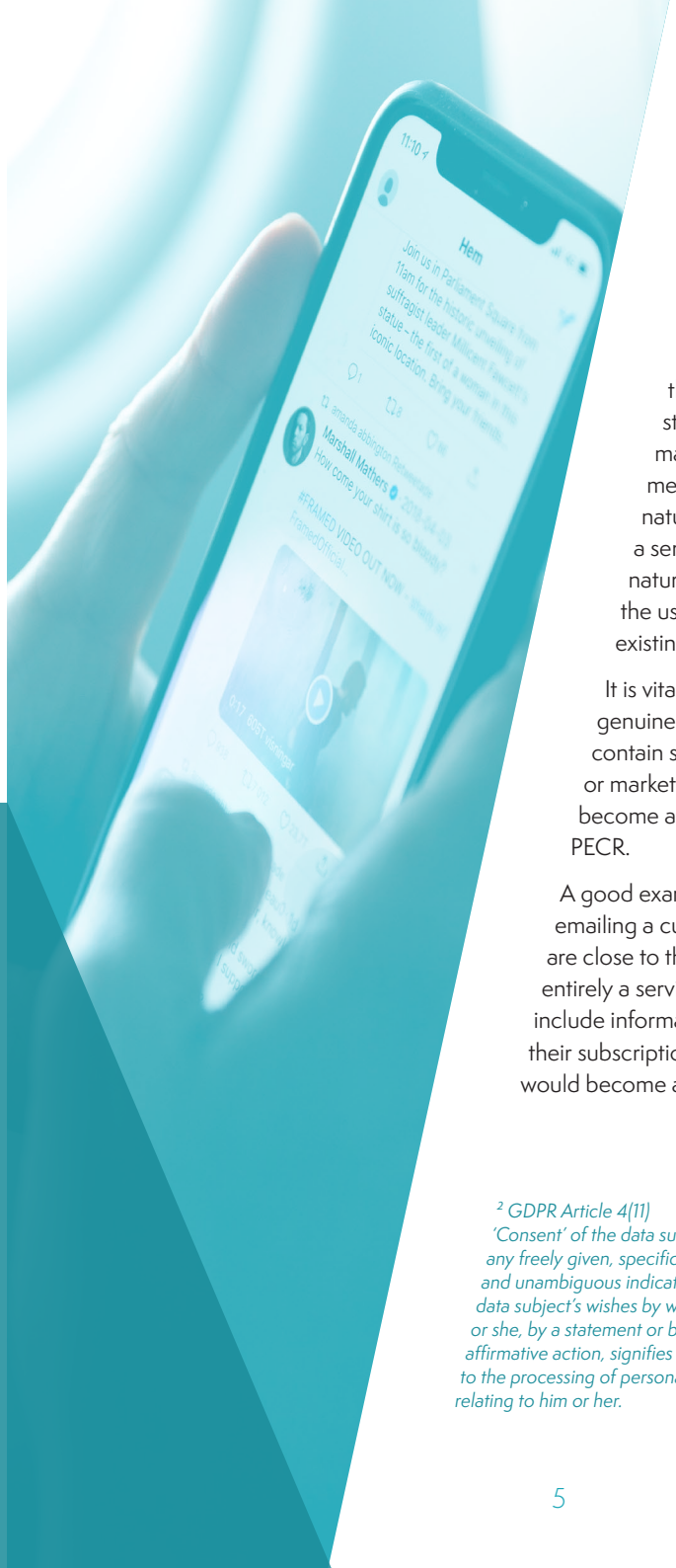
The DPA 2018 mandates that the ICO must draw up a number of Codes of Conduct for specific activities, including Direct Marketing, which then form the basis of assessing compliance with regulations. In the words of the ICO:

> *"If you do not follow the code you will find it difficult to demonstrate that your process complies with GDPR and PECR"*

GDPR covers the law regarding the processing of personal data, whilst PECR covers the law when that data is used to transmit direct marketing messages to individuals electronically (e.g. via email, fax, sms, social media etc). PECR also covers the use of electronic identifiers such as cookies, tracking pixels etc.

Some Direct Marketing activities are not covered by PECR, for instance hard copy material sent through the post, but the processing of personal data for this purpose is still covered by GDPR.

A key area of PECR which changed with the introduction of GDPR was the definition of Consent. PECR now uses the GDPR definition of Consent[2] which must be freely given, informed and affirmative.



MARKETING & SERVICE MESSAGING

PECR draws a distinction between these types of messaging, and only stipulates what must be followed for marketing messaging. A marketing message is one which is promotional in nature and advertises goods or services, a service message is informational in nature and simply provides information the user needs in the context of the existing relationship.

It is vital that service messages are genuinely restricted so that they only contain service information, if any sales or marketing information is included it will become a marketing message and subject to PECR.

A good example would be a telecoms provider emailing a customer to inform them that they are close to their monthly data limit. That is entirely a service message. However should they include information about how they could change their subscription to obtain more data then it would become a marketing message.

[2] *GDPR Article 4(11)*
'Consent' of the data subject means any freely given, specific, informed and 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.

EMAIL MARKETING BASICS

For the sake of simplicity we will refer to email marketing, however remember that these rules apply equally to other digital channels such as SMS (text messaging) or direct messaging on social media platforms, in app messaging or other communication apps, and also includes live (or recorded) telephone calls.

PECR introduces the concept of the "soft opt-in" to Direct Marketing whereby consent is not required to contact an individual who has previously bought (or negotiated to buy) similar goods or services from you in the past. However the individual must be given the option to opt-out **at the time of collecting the data** and on **each and every subsequent email** – in practice this means maintaining a suppression list of individuals who must not receive marketing emails and including an "unsubscribe" button on each email. You should also provide the usual privacy information via a Privacy Notice when you are collecting the personal data. Within the context of GDPR this means that the personal data are being processed for the Legitimate Interest of Direct Marketing, however the individual has the absolute[3] right to Object to this processing and you must respect and uphold that right.

A word of caution for charities and other organisations promoting aims and ideals: the "soft opt-in" applies only to businesses marketing their goods and/or services and does not apply to the promotion of aims or ideals. Where you are marketing to previous donors to solicit further donations you will not have the ability to use the "soft opt-in" and must have instead obtained explicit consent from the individual for this activity.

For individuals who aren't covered by the "soft opt-in" you must obtain their explicit Consent to provide Direct Marketing messages. Once again you must provide an appropriate Privacy Notice, and you must provide them with the ability to withdraw their Consent at any time – which you can do via the same "unsubscribe" mechanism as above. GDPR dictates that the lawful basis of processing the personal data is Consent in this instance, and PECR requires that Consent is obtained for the communications.

From the individual recipient's perspective it is important to understand that the "soft opt-in"/Legitimate Interest justification and the justification of Consent look very similar, and so you should use the same language of "unsubscribe" across both streams. The ICO advises that it would be best practice[4] to utilise specific Consent for both activities regardless of whether the "soft opt-in" applies as this would aid

transparency and understanding amongst individuals. The way this would be managed would be, for example, to provide an "opt in" to marketing activity when the customer buys from you rather than an "opt out".

PECR uses a somewhat archaic term for business to business Direct Marketing and talks of "Corporate Subscribers" to mean business customers[5]. One of the key parts of the Code of Conduct is clearing up some of the rather obtuse language used in the past by the ICO around B2B activities within their PECR guidance. Email Marketing to Business Users and indeed Business Contacts is NOT covered by PECR. However, it is clear that processing personal details such as a business email address unique to the individual would constitute the processing of personal data and so must have a valid lawful basis under GDPR – which would be Legitimate Interest in the absence of specific Consent, however there does not need to be a specific basis to send the Direct Marketing messages. There is also a problem in that sole traders and small partnerships are treated as individuals and not businesses, and so any Direct Marketing activity must be able to identify these correctly and apply the appropriate PECR justification for communicating with them ("Soft Opt-In" or Consent) – in practice this is hugely challenging hence the ICO advice to obtain Consent from all recipients as a best practice is applicable here.

There is also a marketing point to be made here: marketing to people who have provided their consent will return the best results, as they will be more engaged.

[3] Absolute – i.e. cannot be contested, and must be respected and implemented

[4] Note best practice rather than mandated

[5] Because PECR also covers the provision of telecoms services, and was indeed its origin as legislation.

[6] Less than 3 partners

SOURCES OF DATA

The duty to disclose information in a privacy notice when collecting data from the data subject is well understood. However there is a similar duty when you collect data from third parties, including from public records.

If you have, for example, obtained business contacts from an external source then in the privacy notice you supply as part of your marketing communications you must provide the usual privacy notice information plus details of the source of the data[7].

Where you are buying in data it is your responsibility to ensure that the provider of the data has obtained it, processed it and shared it within the bounds of compliance with GDPR. The ICO warns organisations to NOT take assurances of data being "compliant" at face value, and if you have any doubts you should not take the data. There are a set of typical questions supplied by the ICO that you should aim at any potential data vendors to help with vetting them[8]:

- **Who compiled the data** – was it the organisation you are buying it from or was it someone else?
- **Where was the data obtained from** – did it come from the individuals directly or has it come from other sources?
- **What privacy information was used when the data was collected** – what were individuals told their data would be used for?
- **When was the personal data compiled** – what date was it collected and how old is it?
- **How was the personal data collected** – what was the context and method of the collection?
- **Records of the consent (if it is 'consented' data)** – what did individuals' consent to, what were they told, were you named, when and how did they consent?
- **Evidence that the data has been checked against opt-out lists (if claimed)** –can it be demonstrated that the TPS or CTPS has been screened against and how recently?
- **How does the seller deal with individuals' rights** – do they pass on objections?

For B2C businesses buying in personal data for new business marketing you must be satisfied that the individuals have provided consent which **specifically names you** as an organisation they are providing consent for marketing activity to. That consent should have been obtained no longer than six months earlier.

Lastly, once you have purchased new marketing data you should then compare it against your existing data and apply any suppressions / opt-outs that apply where the individuals on the bought in data already exist in your current data.

[7] *GDPR Article 14 https://gdpr-info.eu/art-14-gdpr/*

[8] *Page 53 of the draft Code of Conduct.*

COOKIES ETC

Cookies and other digital technologies such as tracking pixels cannot be deployed to an individual's device unless:

- They are essential for the provision of the online service, or
- Necessary for the transmission of a message (e.g. chat-boxes), or
- The user has provided Consent

It is important when obtaining Consent to ensure that no cookies are deployed in advance, and that full and transparent information is provided to the user so they can make an informed decision. As always, Consent must be as easy to withdraw as to give – so you need to make it easy for people to change their minds.

In practice this means using a cookie management / consent management tool such as CIVIC, however it should be tested and validated before being deployed to a live environment to ensure that it meets the requirements of GDPR and PECR. Specific attention should be given to ensuring that the user is not encouraged to provide consent through any "nudging" techniques, and that cookies have been correctly categorized so that non-essential cookies are not deployed unless consent is provided.

When considering any new technologies such as cookies, tracking pixels etc it would be appropriate to conduct a Data Protection Impact Assessment (DPIA). It is worth remembering that personal data collected by these technologies can be used by the business and potentially the cookie author to enrich personal data with Observed Data and Inferred Data which adds to their profile with information garnered from their wider online behaviour. Hence they must be treated with due caution and a DPIA undertaken.

CUSTOMER RECOMMENDATIONS

The Code of Conduct discuses the likely legality of obtaining personal data from an existing contact of a third party who may be interested in your goods or services – e.g. refer a friend programmes.

There are two ways this can occur:

- Your existing contact gives you the information and you market to the third party
- Your existing contact gives your information to the third party and they contact you

In the ICO's eyes the second route is preferable as the first route is highly unlikely to count as valid consent form the third party to process their data and instigate Direct Marketing for both GDPR and PECR; an individual can not provide consent for someone else.

MARKET RESEARCH

Genuine market research where the communications are sent purely with the aim of conducting research to improve your products and services is not covered by PECR. You would, however, still need to show a lawful basis for processing personal data under GDPR.

The ICO specifically draws attention to the practice of "Sugging" – Selling Under the Guise of Research. If any attempt is made to market or sell your products and services within the process of conducting the research, or to retain the data obtained for future marketing activity then the whole activity would fall within the remit of PECR and you must include details of the processing associated with the marketing activity within any supplied Privacy Notices.

As an aside, if you discover errors within your data as a result of research activity (a data subject's name being incorrectly spelled for example) then your duty of maintaining data accuracy would apply and you should amend your data accordingly.

SOCIAL MEDIA MARKETING

There are two main forms of social media marketing:

- Uploading personal data from your records to find matches within a social media platform to add them to a group on that platform and then market to them. Examples of this would be Facebook Custom Audiences or LinkedIn Contact Targeting, and
- Creating "lookalike" audiences where there is no direct relationship with the data subjects but the platform takes a profile from you to create an ideal profile which is then applied to their users who receive in platform marketing

For the first of these routes the ICO is clear that Consent is the only likely basis for sharing your data with the platform, who would then be acting as a Joint Controller. This means you must obtain consent from each individual to share their data with the platform and be clear on this within your Privacy Notices.

For the second scenario you are not necessarily sharing any personal data with the platform per se and so this route carries a reduced overhead.

You should however be aware that these campaigns frequently use technologies such as tracking pixels which will need specific Consent (see cookies above). Also you should satisfy yourself that the social media platform has taken all necessary steps to be transparent and that you can direct enquiries from individuals to the correct privacy information on their site.

SPECIAL CATEGORY DATA

Using special category data (i.e. data related to race, body, belief or sex) for direct marketing purposes is lawful provided you have the Consent of the data subject. No other lawful basis within either GDPR or PECR is valid.

CONCLUSIONS

The draft Code of Conduct is designed to limit unlawful activity and provide a framework for the legitimate activity of marketing a business.

The PECR regulations are somewhat dated and originate from a time which pre-dated much of the technology which is prevalent today (for example it has a lot to say about marketing via fax – which is a tad unpopular these days), and so uses a number of outdated terms which the Code of Conduct seeks to clarify and redress.

GDPR, PECR and the draft Code of Conduct do not prevent you from marketing your goods and services. However they do have a number of key messages which are consistent and which you should follow, specifically:

- **Be transparent and informative in the privacy notices you supply**
- **Obtain consent where required. If in doubt it is better to obtain it than try to adjust another lawful basis to fit**
- **The right to object to direct marketing is absolute and you must respect the individuals request to be excluded –you must always provide an "unsubscribe" option to all marketing messages**
- **B2B marketing is valid, and excluded from the requirement of Consent for that first email message. You should however seeks to obtain consent wherever possible as a best practice, and in all cases include an unsubscribe on every message.**
- **PECR has nothing to say about marketing through the post, as long as you comply with GDPR for processing personal data**
- **Separate out service messages from marketing messages**
- **For new marketing projects, especially ones using new channels, agencies or suppliers, you should undertake a Data Protection Impact Assessment (DPIA)**

About GDPR Assist

GDPR Assist is the trading name of Paul Strout, a Bury based Data Protection Practitioner with many decades experience in helping organisations with their key operational processes.

More information is available at **www.gdprassist.co.uk**

Designed by: www.outflux.co.uk