A Data Protection guide to the use of marketing data

In view of recent ICO enforcement action, **Dr Nathalie Moreno** of Lewis Silkin LLP explains how the rules under the DP Act, PECR, GDPR and DMA Code affect companies' direct marketing operations.

This data protection guide serves as a tool for marketers facing a plethora of evolving laws and guidelines on the processing of personal data. With the EU General data Protection Regulation (GDPR) due to come into force in 2018, it is important that advertisers and marketers prepare themselves and ensure that their marketing practices are forward-looking and compliant.

In this article, we aim to address the following issues:

- What is direct marketing?
- How can the data be used?
- What cannot be done?
- What happens when it goes wrong?

What is direct marketing?

Direct marketing is defined under the Data Protection Act 1998 (DP Act) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) as:

1. The communication **(by whatever means)** ….
2. of **any** advertising or marketing material….
3. which is **directed** to **particular individuals**.

The definition is broad and can include (but is not limited to) phone calls, emails, online marketing and texts, and applies even where the main purpose of the communication is not marketing. It covers both commercial and non-commercial marketing material including promoting the aims of non-profit organisations, political parties as well as incidental marketing or advertising such as offering other products or services on phone calls or emails, even where the primary purpose of the call or email was not for marketing.

The third part of the definition is crucial in that it must be targeted at particular individuals, for example by name or email. Blanket marketing such as distribution of leaflets on a high street, will therefore, not be covered.

Market research: The direct marketing rules do not apply to market research. However, any personal data gathered for market research purposes must be processed fairly, securely and only for research purposes. The market research must be genuine, and not used as a cover to sell goods or services or collect data for marketing purposes.

The DMA (Direct Marketing Association) Code also requires that when members collect personal information for the purposes of research or a survey and also intend to use this information for any other purpose, such as to market to consumers, they must make this conspicuously clear. They must not misrepresent themselves as carrying out research or a survey when the real purpose of the contact is to sell goods or services, or to solicit donations.

> The GDPR requires that consent is unambiguous and contains a statement or clear affirmative action.

How can the data be used?

There are several categories of marketing which have different rules.

Solicited marketing: There is no restriction on communication of marketing where an individual has specifically requested the marketing material. However, the communication must only be in relation to the specific request.

Unsolicited marketing: The Privacy and Electronic Communications Regulations (PECR) applies and therefore if an organisation sends any message to a customer which has not been actively requested (even if they have "opted-in" to receive the messages) the organisation must state who they are, provide contact details to enable the individual to opt out of the marketing and allow their number to be displayed to the person receiving the call. Generally speaking, consent is also required, as outlined below.

Consent: According to the DP Act, consent must be:

1. **Freely given** – organisations should not coerce or improperly incentivise individuals to consent to marketing, or penalise those who do not give consent.
2. **Specific** – if the marketing sent to the individual has not been specifically requested, this will be seen as unsolicited and is capable of sanction. This will be the case even where the individual has opted-in to marketing when the opt-in request is not sufficiently specific.
   Organisations cannot share data with group companies or third parties without seeking specific consent from the individual to do this. At present, organisations should name the class of third party with whom they intend to share that data. Once the GDPR comes into force, organisations may be required to name the third party specifically.
   Likewise, organisations should not use personal data sent to them by a third party without verifying that the third party collected the data in accordance with the legislation set out above and, preferably, without verifying that the third party notified the individual that it would be passing their personal data to the organisation and the purpose for

which the organisation would use it.
3. **Informed** – in setting out how the individual's data will be used, the notice cannot be too dense or difficult to find; and
4. given by a **positive action** from the individual; organisations cannot assume consent from a failure to opt-out unless this is part of positive action.

The GDPR requires that that consent is unambiguous and contains a statement or clear affirmative action. It requires granular consent for distinct processing operations and should be separate from other terms and conditions. It also gives a specific right for the individual to withdraw their consent. Organisations must inform individuals about their right to withdraw, and offer them easy ways to withdraw consent at any time.

The individual must also have a genuine choice over whether or not to consent and should not be coerced or unduly incentivised to consent, or be penalised for refusing. If consent is a condition of subscription to a service, the organisation must demonstrate how consent was freely given. Consent must also be specific to the type of marketing communication in question and organisations must make sure that they clearly and prominently explain exactly what the person is agreeing to, if this is not obvious.

Consent must be a positive expression of choice. It does not 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 organisations cannot 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.

Withdrawal of consent: If an individual withdraws consent by notice in writing, the organisation must stop marketing within a reasonable period. The ICO guidance suggests in most circumstances they expect that calls, texts or other electronic communications should stop within 28 days of receiving the objection, and postal communications should stop within two months. And if the organisation can reasonably stop sooner, it must.

Electronic marketing messages: There is an additional PECR requirement for electronic marketing messages that "the [recipient] has previously notified the [caller or sender] that he consents for the time being to such communications being sent by, or at the instigation of, the [caller or sender]". This requires that:

1. The recipient has notified the sender (i.e. the organisation cannot rely on third party or indirect consent where the individual has originally given the consent to another organisation, unless the person intended their consent to be passed on to the organisation undertaking the marketing); and
2. Consent is 'for the time being' i.e. ongoing as long as circumstances remain the same, and will expire if there is a significant change in circumstances.

Opt-in: Where an individual has ticked a box opting-in to future marketing, the marketing is still unsolicited and therefore PECR rules apply; however it is likely to be lawful because it may constitute consent under the PECR. Opt in boxes must:

> If consent is a condition of subscription to a service, the organisation must demonstrate how consent was freely given.

1. Be specific to each type of electronic marketing. For example:
   "Tick if you would like to receive information about our products and any special offers by post / by email / by telephone / by text message / by recorded call".
2. Use language that is clear and easy to understand.

The GDPR specifically bans pre-ticked opt-in boxes.

Opt – Out: Failure to tick an opt-out box does not automatically constitute consent, therefore opt-in boxes are preferable. Where opt-out boxes are used they should be prominent, use clear language and be easy to understand. For example:

By submitting this registration form, you indicate your consent to receiving email marketing messages from us. If you do not want to receive such messages, tick here.

Third party and indirect consent: ICO guidance indicates that where an organisation is using a bought-in marketing list, the consent would have been granted to another organisation and is unlikely to be valid, particularly if the consent was general, for example consenting to marketing from "selected third parties". Under the GDPR, the ICO suggests that even specifying precise and defined categories of organisations within the consent may not be sufficient for consent to be valid. It is best to name the third party who will be relying on it.

The DMA Code places an obligation on members to satisfy themselves, when buying or renting personal data, that the data has been properly sourced, permissioned and cleaned.

Other obligations: The DMA Code requires members to operate and maintain an in-house suppression file – listing the names and contact details of consumers who have indicated they do not wish to receive commercial communications via all or particular means of communication. This includes recipients of third-party communications who have indicated at the first contact that they do not want to receive further communications.

Members must also ensure that lists containing names and contact details are not used for marketing purposes unless the list has been cleaned against the relevant preference services – Telephone Preference Service (TPS), Mailing Preference Service (MPS), Corporate Telephone Preference Service (CTPS), Baby Mailing Preference Service (BMPS), Facsimile Preference Service (FPS) and Your Choice for unaddressed mail from DMA members[1].

The Code requires members to comply with four core principles:

1. **Respect Privacy:** This involves taking all reasonable steps to ensure consumers do not receive commercial telephone calls or SMS messages at times considered to be

antisocial. Members must screen data to remove files of deceased people so that they are not used for marketing. Members must not undertake random number or sequential dialling, whether manually or by computer, or any number scanning activities (any activity designed to establish the validity of telephone numbers).

2. **Be honest and fair:** Members must also be open, transparent and honest and take particular care when dealing with children and other vulnerable consumers. They must clearly identify the advertiser on any one-to-one marketing communication that they send or instigate and must provide caller line identification, to which a return call can be made, whenever they undertake any outbound calls. They must also provide a valid address on any marketing communication, through which the consumer can opt out of future communications.

   Members must not send goods or provide services for which payment is requested to any consumer without first having received an instruction to supply such goods or services and must not demand that any consumer either pay for or return unsolicited products, except for substitute products. Members must not adopt high-pressure selling techniques in the course of any contact with any consumer or business.
3. **Be diligent with data:** The DMA Code requires compliance with the DP Act and PECR but reinforces this point by explaining that when collecting personal data, either on or off line, to be subsequently used for one-to-one marketing purposes, members must do all of the following:
   - Clearly identify themselves or the party collecting the data;
   - Specify the purpose for which this personal data is to be used – unless this is obvious from the context or the consumer already knows; and
   - Identify any further information necessary to enable the processing to be fair.

   Any personal data collected should be adequate, relevant and not excessive for the purpose for which it has been collected. Personal data should be accurate and up to date and should not be kept for longer than necessary for the purpose for which it has been collected.

   Members should ensure that they have **appropriate technical and organisational measures** to ensure data is not processed unlawfully or without authority and is protected from accidental loss, destruction or damage. If they transfer personal data outside the European Economic Area (EEA), there are adequate levels of protection for the rights of the consumer.

   Where a member acts as a data processor and collects data on behalf of a data controller, this must be carried out under contract. Members must not use 'sensitive' personal data for marketing purposes without the explicit consent of the consumer concerned.
4. **Take responsibility:** Members must act decently, fairly and reasonably, fulfilling their contractual obligations at all times. Members acting as an agency or supplier for a non-member's one-to-one marketing activity must advise the non-member to act within the Code. If the non-member client does not take that advice, the member must insist as a condition of acting for the non-member that the Code is followed in respect of all relevant work. Where members subcontract work to non-DMA members, they must ensure that the contractor complies with the Code in respect of the sub-contracted work – and must accept responsibility for the consequences of non-compliance by the contractor.

   Members must maintain adequate records to demonstrate compliance with the Code – and must maintain an adequate system of monitoring and audit. Failure to accept such recommendations may result in a referral to the Direct Marketing Commission (DMC) for adjudication and, where such adjudication is negative, to sanctions for a breach of the Code.

What cannot be done?

Organisations must not market to individuals without consent (see above).

They also must not:

- Market to individuals unnecessarily. What is "necessary" is defined narrowly in the DP Act and is rarely applicable;
- Market when not within the legitimate interests of the company. Broadly, an interest will be legitimate where it is lawful, clearly articulated and a real and present interest;
- Avoid direct marketing rules by framing the correspondence as market research when in fact their intention is to sell goods or services or collect data to be used for marketing purposes at a later date;
- Email or text an individual to seek consent to future marketing messages. This in itself is sent for the purposes of direct marketing, and is therefore subject to the legislation set out above.

What happens when it goes wrong?

The ICO is responsible for enforcement of the DP Act and PECR and has the power to take enforcement action when direct marketing legislation has been breached. At present, the ICO can:

- issue an Enforcement Notice requiring organisations to remedy a breach (note that failure to respond to this notice is a criminal offence);
- issue monetary fines of up to £500,000 for serious breaches.

Once the GDPR comes into force, these fines could increase up to €20 million or 4% of global annual turnover of a business, whichever is higher. As such, and given the fact that the ICO is increasingly issuing fines after receiving one isolated complaint from a member of the public, organisations should ensure that they are acting in compliance with all current and future data protection legislation.

In two recent decisions, set out below, two well-known companies were hit with hefty fines in attempting to align their marketing practices with the upcoming legislation.

- **Flybe** was fined £70,000 for sending over 3.3 million emails to individuals who had told them they did not want to receive marketing emails from the company. The email asked recipients to check that the details held by Flybe were correct and that any marketing preferences were updated.

- **Honda** was fined £13,000 for sending an email to over 280,000 individuals intending to clarify the marketing preferences of recipients. Honda argued that these emails were customer service emails helping them to comply with data protection legislation. However the company could not demonstrate that the recipients had ever consented to receiving this type of email.

The ICO has recognised that organisations will be reviewing their marketing practices in preparation for stricter regulation under the GDPR. However Steve Eckersley, Head of Enforcement at the ICO warned that "businesses must understand they can't break one law to get ready for another".

AUTHOR

Dr Nathalie Moreno is a Partner at Lewis Silkin LLP (Technology, Commercial and Data Privacy).
Email: Nathalie.Moreno@lewissilkin.com

REFERENCES

1 See corporate.tpsonline.org.uk/ and www.mpsonline.org.uk/mpsr/yourchoice/

ICO issues GDPR draft guidance on contracts

The ICO's document, published on 13 September and currently open for consultation, explains contracts and liabilities between controllers and processors under the GDPR. The ICO says that contracts must state details of the processing, such as the nature and purpose of the processing, the type of personal data and categories of data subject, and must also set out the processor's obligations. This includes the standards the processor must meet when processing personal data and the permissions it needs from the controller in relation to the processing.

In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However, at the moment no standard clauses have been drafted.

"Data controllers are ultimately responsible for ensuring that personal data is processed in accordance with the GDPR. This means that, regardless of your use of a processor, you may be subject to any of the corrective measures and sanctions set out in GDPR. These include orders to bring processing into compliance, claims for compensation from a data subject and administrative fines. Further guidance on sanctions and corrective measures under the GDPR will be issued in due course."

"Unless you can prove that you were 'not in any way responsible for the event giving rise to the damage', you will be fully liable for any damage caused by non-compliant processing, regardless of your use of a processor."

Processors can also be held liable under Article 82 to pay compensation for the damage caused by processing if they have failed to comply with the GDPR provisions specifically relating to processors, or if they have acted without the lawful instructions of the controller, or against those instructions.

The consultation ends on 10 October. The ICO intends to publish the final version of the guidance later in 2017.

- *See ico.org.uk/about-the-ico/consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/*

ICO: GDPR means no change in appetite for fining

The government's statement of intent in August to legislate in GDPR-style also confirmed GDPR-level fines, but the Information Commissioner, Elizabeth Denham, says that maximum fines will not become the norm.

Writing in a blog, Denham states that issuing fines has always been, and will continue to be, a last resort: "We have never invoked our maximum powers. Predictions of massive fines under the GDPR that simply scale up penalties we've issued under the Data Protection Act are nonsense."

Denham says that the ICO intends to use new GDPR powers proportionately and judiciously.

"Like the DP Act, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow."

Commenting on the government's plans, Denham said: "We are pleased the government recognises the importance of data protection, its central role in increasing trust and confidence in the digital economy and the benefits the enhanced protections will bring to the public."

- *See Elizabeth Denham's blog at iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/#more-2853*

Charities' attitudes vary on cyber security

A recent study commissioned by the Department for Digital Culture, Media and Sport (DCMS) reveals that charities' attitudes to cyber security range from regarding it as a serious issue to considering it an unaffordable luxury.

According to the authors of the report, there is a need for basic awareness-raising among staff and trustees, and training of those responsible for cyber security. The Ipsos MORI research is based on 30 in-depth interviews.

- *See www.gov.uk/government/uploads/system/uploads/attachment_data/file/635593/Cyber_security_among_charities_-_findings_from_qualitative_research_-_DCMS.pdf*

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The future of data protection law and enforcement in light of Brexit

In the summer, the government expressed its thoughts about the UK's future DP law. **Nicola Fulford** and **Gemma Lockyer** of Kemp Little LLP look at the derogations from the GDPR.

On 23 June 2016, the United Kingdom voted to leave the European Union and whilst that leaves us in a period of uncertainty in many respects, we have received some guidance as to where the UK's data protection law and strategy is going. On 7 August 2017 the Department for Digital, Culture, Media and Sport published their statement of intent for the planned reforms that will form the new Data Protection Bill (Statement of Intent). The Data Protection Bill will bring

Continued on p.3

Woodland Trust turns over a new leaf in collecting consent

The charity reviewed the design and presentation of opt-in to ensure increased and better quality consent. By **Laura Linkomies**.

Woodland Trust, a charity with over 500,000 members and supporters and more than 1,000 sites (woods) all over the UK, had previously presented consent statements as an "obligatory"tick box – just like many others. In May last year, the organisation decided to re-think its strategy. It was felt that a new, tailored consent wording, written from an appealing marketing perspective rather than solely a legal requirement, would serve members and supporters better.

Melanie Sallis, Head of Supporter Marketing at Woodland Trust

Continued on p.5

Issue 93 **September 2017**

UNITED KINGDOM
report

ISSUE NO 93 **SEPTEMBER 2017**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan.thomas@privacylaws.com

CONTRIBUTORS

Rebecca Cousin
Slaughter and May

Alison Deighton
TLT LLP

Nicola Fulford and Gemma Lockyer
Kemp Little LLP

Nathalie Moreno
Lewis Silkin LLP

Robert Waixel
PL&B Correspondent

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Data Protection Bill introduced in House of Lords

The government issued its statement of intent in the summer and we now have an indication of how it intends to use the derogations allowed for in the GDPR (p.1). As we go to print, we now have a DP Bill (p.6) but one of the sticking points with regard to data transfers abroad will be the Investigatory Powers Act. Will the UK be seen as adequate? Remember that Jersey, Guernsey and the Isle of Man have based their legislation on the current UK DP Act and all of them have obtained an adequacy decision. A further point is that the government's paper (p.7) states "The UK's data protection standards will remain fully aligned with the revised Convention 108." However, the UK has not ratified the Additional Protocol, dated 2001.

Whilst organisations are waiting for more guidance in several areas, data security is something that can be addressed now. The GDPR helpfully provides guidance on how organisations can address security issues "appropriate to the risk". These measures include pseudonymisation and encryption. But, as Paul Maskell of Bluelightsdigital told the Data Protection Forum last week, it is important to present GDPR as an opportunity and frame it positively. Read on pp. 19-20 about a company where privacy compliance is expanding from being a legal issue to a governance one.

A DPO appointment may not be mandatory but those who need to appoint one will have several aspects to consider (pp. 8-10). Sometimes, a risk assessment is needed to establish whether a DPO is needed. Another GDPR issue that is still problematic is seeking consent and documenting it properly. Read on p. 1 how Woodland Trust revamped its processes around consent to make sure individuals are aware what they are consenting to. Further on this topic, read on p.15 tips on using data within the law when conducting marketing campaigns.

We are also pleased to bring you insights into the win-win benefits of embracing an FOI culture in Buckinghamshire (pp.21-23). If you would like to be interviewed about how your company is preparing for the GDPR or complies with the current law, please contact me at laura@privacylaws.com

Last but not least, read about the pros and cons of personal data stores – individuals "taking back control" (pp. 11-12).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business* Reports. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. **Steve Wright, Chief Privacy Officer, Unilever, UK**"

Subscription Fees

Single User Access

UK Edition **£440 + VAT***

International Edition **£550 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2-year (10%) and 3-year (15%) subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int