LEGAL GUIDE TO DATABASE MARKETING

Overview

Database marketing is a form of direct marketing that uses electronic databases of customers to generate targeted lists for direct marketing communications. This process is all about identifying, collecting and then analysing relevant information about a company's customers (and potential customers), to allow brands to improve their products and services, to build better marketing strategies and – ultimately – to customise the conversations and develop the relationships that they have with individual customers. These databases may include a very wide range of personal information about customers, including names, addresses, phone numbers, e-mail correspondence, purchase histories, and prior information requests and subscriptions. Databases like these may very well contain data that can (and has been) be legally collected and legitimately used, and may further be augmented (or "enriched") by leveraging the vast amount of information available via digital media sources and social media platforms.

Legislation

This guideline is compiled to assist advertisers and marketers navigate their way around the use and management of databases (or "electronic databases" as they are often referred to in South African law). Businesses and practitioners need to understand the law governing databases, to know the restrictions and limitations that apply to the use of the information that they hold and to understand their obligations in relation to such information.

What are electronic databases?

> *"Electronic databases are collections of recorded data or information in an electronic or digital form."*

A good database will be up to date, accurate, and will hold reliable records of specific consent to receipt of marketing communications given by the "data subject" (the person about whom information is held). Such a database can be used in compliance with the law and should generate few queries or complaints. However, where a database is out of date, inaccurate, and contain details

of people who have *not* consented to their information being used or disclosed for marketing purposes, the organisation risks facing regulatory penalties (as well as criminal sanctions for senior management) and sets itself up for serious reputational risk. Examples of such databases range from marketing leads to internal staff information databases.

In South Africa, the laws impacting databases are the following:

- The Copyright Act 1978

Understanding copyright law helps identify the author and owner of the database. The key question is whether a new "work" has been created to which rights of authorship/ ownership can be attached. Section 1(1) of The Copyright Act defines a "literary work" to include:

> *"tables and compilations, including tables and compilations of data stored or embodied in a computer or a medium used in conjunction with a computer".*

South African law is clear about the protection of electronic databases as a compilation and as a class of literary works, may therefore receive copyright protection.

The requirement of originality applies to databases, and so a database must be independently compiled and the arrangement of the data in the compilation itself must evidence originality in order for copyright to vest in the author. A database that is copied is not original. All compilations, however, constitute original works of authorship in themselves. The international *Berne Convention for the Protection of Literary and Artistic Works* confirms the South African approach and grants copyright protection to collections of literary or artistic works because of the selection and arrangement of their contents. Electronic databases therefore domestically and internationally constitute intellectual creations.

An important consideration to understand is the difference between the "maker" (author) and "first owner" of a database. The person who invests in the creation of the database and works on the contents of the database is usually the "maker" and the first owner of the database right. Where the creation of a database is *commissioned*, then the commissioning party will usually be the "maker" and first owner of the database right, even though someone else performed the actual task of putting it together. If the database is made by an employee in the course of his employment, the employer will be regarded as the maker and therefore the owner of the database right.

Like other forms of intellectual property, the use of a database is usually granted by its owners by way of a licence. Alternatively, ownership of the database may be transferred by the owner to another person by way of assignment. In terms of South African copyright laws, any assignment of copyright (including copyright in a database) must be in writing. This means that the owner of the copyright has the option of licensing the use of the database to a third party (in return for payment of a royalty) and retain ownership of the copyright in the database, or he/she can assign the copyright to a new owner (for a price). The implications of the latter are that the new owner has exclusive rights regarding the copyright of the database. The first owner (or author) will then lose all rights associated with it.

➢ The Protection of Personal Information Act 2013 ("PoPI")

With the enactment of PoPI, the concept of "Personal Information" has finally be defined. The definition is incredibly wide and covers the following elements:

1. Race
2. Gender
3. Sex
4. Pregnancy
5. Marital status
6. National, ethnic or social origin
7. Colour
8. Sexual orientation
9. Age
10. Physical or mental health
11. Well-being
12. Disability
13. Religion
14. Conscience
15. Belief
16. Culture
17. Language
18. Birth of the person
19. Education
20. Medical
21. Financial
22. Criminal history
23. Employment history
24. Any identifying number, symbol
25. e-mail address
26. physical address
27. telephone number
28. location information
29. online identifier or
30. other particular assignment to the person
31. the biometric information of the person
32. Blood type
33. Personal opinions
34. Views
35. Preferences
36. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
37. Views or opinions of another individual about the person
38. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

PoPI grants protection to the elements listed above and is clear that the use of any of the elements must be with the express consent of the individual to which it relates. To "Process" (collect, retain, store, use, share or destroy) any Personal Information held in an electronic database means that an organisation should have specific consents from the person for the specific act of receiving marketing communications. Under PoPI, database marketing entails the storing of specific consents, for receiving marketing communications from the organisation, from each individual listed in the database.

➢ The Electronic Communications and Transactions (ECT) Act 2002

For database marketing, targeted lists are drawn and marketing communications are sent to consumers. Section 45 of the ECT Act is clear that where unsolicited commercial communications are sent to consumers, the consumers must have the option to unsubscribe from the mailing list and the consumer must be informed as to how their details were obtained by the mailer. The penalty for unsolicited communications is a fine or imprisonment for a period not exceeding 12 months.

➢ Consumer Protection Act (CPA) 2008

The CPA contains sections that are designed to provide the consumer with the tools to prevent unsolicited direct marketing communications. Consumers are afforded various rights that are aimed at protecting them from unwanted marketing material whilst limitations are placed on marketers regarding their business practices. The CPA defines direct marketing as:

> *"approach[ing] a person, either in person or by mail or electronic communication, for the direct or indirect purpose of-*
>
> *a. promoting or offering to supply, in the ordinary course of business, any goods or services to the person; or*
> *b. requesting the person to make a donation of any kind for any reason".*

In addition, the Act provides the meaning of 'electronic communication' as:

> *"communication by means of electronic transmission, including by telephone, fax, SMS, wireless computer access, email or any similar technology or device".*

In 2011, a set of Regulations were enacted to support the CPA. The Consumer Protection Act Regulations ("Regulations") expanded upon various issues pertaining to direct marketing and as such have an impact on the use of databases for marketing purposes. Part 4 of the Regulations state that:

> *"if a consumer has -*
>
> *(a) informed the direct marketer; or*
>
> *(b) placed any communication or sign on a postal box, post office box or other container for mail,*

indicating that he or she does not wish to receive any material related to direct marketing, then the direct marketer -

> *(i) may not place or attach any material primarily aimed at direct marketing, in whichever physical format, in or on or near the postal box, post office box, container, or in, on or near the fence, gate or any other part of the premises of the consumer; and (ii) must provide the consumer with written confirmation of the receipt by the direct marketer of the notice referred in paragraph (a) above".*

The implications of these Regulations is that the right afforded to consumers with regard to *blocking* unwanted marketing communications is given substance. The marketer is mandated to behave in accordance with the Regulations if the consumer chooses not to receive any direct marketing material.

Buying and selling a database

When the owner of a database intends to allow others to access a marketing database, it must do so in compliance with the law. As discussed above, the owner of a database may licence the database or assign all rights in the database. Additionally, considering that the database contains personal information, the seller must have obtained the necessary consent from the data subjects listed in the database to convey their details to third parties.

The purchaser of the database should query whether the database owner is authorised to sell the database; has informed the data subjects of how their information will be used/processed, obtained the consent of the data subjects where necessary and has the requisite consent to convey the personal details of the data subjects. This means that the individuals listed in the database must have fully understood the purpose and details of the processing of their personal information and provided explicit consent that is required for further processing by a third party as well as use of their personal information for marketing purposes. Any requests to opt-out from direct marketing needs to have been effected by the seller and the personal details of such person should not be used for direct marketing. Records of express opt-ins to receive direct marketing, where applicable should be provided to the purchaser of the database.

Opting Out

With the implementation of the Consumer Protection Act (CPA), the manner in which consumers could be contacted directly is heavily regulated. This applies to situations where the consumer's contact information was obtained via a database. The most relevant implication of this Act, is that it mandated the creation of a system where consumers or potential consumers are to be provided with the option to 'opt-out' from being contacted further (for direct marketing purposes). Additionally, exercising the right to opt-out is to be free of charge.

The Section 11(1) of the CPA states the following:

> *"The right of every person to privacy includes the right to-*
>
> *a) refuse to accept:*
>
> *b) require another person to discontinue; or*
>
> *c) in the case of an approach other than in person, to pre-emptively block,*
>
> *any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing".*

In addition to the opt out mechanism, the CPA stipulates the creation of a registry which was to be created by the National Consumer Commission (NCC). The purpose of this registry is to allow consumers the ability to register their choice to opt out from receiving direct marketing material from a specific supplier or in general. Marketers would then be obliged to align their databases with the registry (implementing specific opt-outs) before initiating a direct marketing campaign. If there is doubt as to whether an individual has opted out from receiving direct marketing material, it must be assumed that he/she has opted out until proven otherwise. An exception exists to this rule and that where an existing consumer has provided prior consent to the marketer to receive direct marketing material.

Opting In

With the introduction of the Protection of Personal Information Act (PoPI), electronic direct marketing practices were re-examined. It must be noted that the CPA applies to both electronic

and non-electronic marketing where as PoPI only applies to electronic marketing. This is made clear in section 69(1) of PoPI. From this, it is evident that PoPI's application is much more specific than that of the CPA. As such, in circumstances of direct electronic marketing, PoPI applies. In all other instances of direct marketing, the CPA applies. In cases where it would appear that both PoPI and the CPA are applicable, the statute which provides the consumer with the highest level of legal protection is applied. Determining which Act applies will need to be determined on a case by case basis.

PoPI introduces an 'opt-in' system as opposed to the CPA's 'opt-out' system. The major difference is that subject to exception, PoPI mandates marketers to receive consent form the potential consumer first before engaging in direct marketing practices. Meaning that the consumer must consent (or opt-in) to being contact directly for marketing purposes. It is important to highlight the consent requirements stipulated by PoPI. The data subject must provide consent for their personal information to be processed and they must consent to receiving direct marketing material. This means that two instances of consent must be elicited from the consumer.

Section 69 of PoPI states the following:

> *"(1) The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—*
>
> *(a) has given his, her or its consent to the processing".*

An exception exists to the prior consent requirement, namely where the consumer is an existing consumer who has provided their personal information to the supplier for the purpose of direct marketing. An important caveat to add is that the consumer must have been provided with adequate opportunities to object to being contacted directly or having his/her personal information used for this purpose. Marketers are afforded a concession, namely they may contact a consumer once in order to obtain consent to contact further.

DMA National OPT OUT Database

The Direct Marketing Association (DMA) has established a private database that maintains a record of consumers who have registered their choice to opt-out from receiving communications for marketing purposes. Members of the DMA have access to the database and will not contact consumers directly who have opted to not receive marketing communications. It is important to note that members of the DMA do not have access to the personal information of registered users. See https://www.nationaloptout.co.za/ for more information.

Retention

An important aspect of databases is the reason, relevance and retention period of the personal information. PoPI requires that personal information held must be relevant and not excessive, up to date and for the purpose for which it was gathered. Section 14(1) of PoPI says that records of personal information must not be kept any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed. As an example, if personal information has been gathered to provide a consumer with a service, such as access to a website, then that consumer's personal information can only be retained for as long as he/she remains a user of said service. However, section 14(1)(a) sets out a number of exceptions to this requirement. These include: retention that is required by law and consent by the data subject to the retention. Retaining personal information for a longer period of time can be done for historical, statistical or research purposes. The Act adds the caveat that this will only be allowed if adequate safeguards are in place to prevent misuse of the information. Any information that is no longer allowed to be used must be deleted, destroyed or de-identified.

PoPI places a heavy emphasis on informing the data subject of his/her rights when it comes to personal information. As such, section 23 of the PoPI allows for a data subject to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the him/her. Additionally, the data subject can request from the responsible party the record or a description of the personal information about the data subject held by the responsible party.

According to section 24 of PoPI, a data subject may request a responsible party to correct personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. When personal information falls into these categories will need to be determined on a case by case basis.

Practical Guidance

The following 5-point Checklist developed by an international law firm[1] is a practical means of assessing the legal position, particularly the rights of ownership and use, of databases:

1. Review any databases that potentially qualify for protection.

- ¬ Do they attract copyright/database right protection?
- ¬ Who is the owner of the databases? Consider whether there are any licences to use the databases and/or whether an assignment of the rights in such databases could be obtained.

2. Review contracts relating to commissioned databases and employment contracts. Also review any contracts where a database may be created and/or enhanced as a consequence of providing a service (such as a customer database created in the context of a sales agency) where the ownership position may not be clear.

- ¬ Do these contracts deal expressly with ownership/assignment of copyright and database rights?

3. Update databases regularly to ensure the 15-year protection period recommences.

4. Protect against infringement by using copyright notices (© [Owner] [Year] All rights reserved) and some text to the effect that the set of data may be protected by database right.

5. Keep a record of the "financial, human or technical resources" put into a database as proof of substantial investment, and be sure to make separate investment in the organisation and arrangement of the database itself in addition to any investment in the creation the data

[1] Source: http://www.out-law.com/page-5698