



DMA Best Practice Guidelines

DATA IN DIRECT MARKETING



Contents

Introduction

DM Code Definitions

Why Best Practice?

Section A

Data Protection and Related Legislation

Section B

Caring for Personal Data

Section C

Data Capture

Section D

Receipt and Transfer of Data

Section E

Name and Address Conversion and Cleaning

Section F

Name and Address Cleaning

Section G

Deduplication and Merge-Purge

Section H

Screening

Section I

Data Tagging and Enhancement

Section J

Sortation and Output

Section K

Appendix – Useful Addresses



Introduction

The contents of this document are designed to address the common issues that may occur and provide guidelines to avoid mistakes and advise on best practice for use of data in direct marketing.

Best practice means the standards, which it is desirable for all those involved with data to achieve. Members of the DMA are already required to comply with the Association's Code of Practice as a condition of membership. Best practice guidelines go beyond these levels by establishing benchmarks for members to aim at in the way they hold, handle and use data.



The following definitions come from the DM Code of Practice (3rd Edition), which is written and published by the Direct Marketing Association.

DM Code Definitions:

"data" is information which:

a) is processed, or is recorded with the intention that it should be processed, by means of equipment operating automatically in response to instructions given for any direct marketing purposes, however it is accessed and whether or not it is in the form of a list

b) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system (i.e. manual data where data is structured in such a way that specific information relating to a particular individual is readily accessible).

"personal data" is information from which a living individual can be identified, whether from that information alone or combined with other information, which is in the possession of, or is likely to come into the possession of, the data controller. Members should be aware that information might be personal data even where an individual is not named, if it is possible to identify that person using information obtained from other sources. Business information and email addresses from which a living individual may be identified are also regarded as personal data and are covered by these rules.

"data controller" is a person or organisation who, either alone or jointly, determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

"data subject" is an individual who is the subject of personal data.

"data processing" is collecting or storing information or data or carrying out any operation/s on the information or data.

"data processor" is a person who collects, stores or deals with personal data on behalf of a data controller (including a list broker/manager).

"data supplier" is a data controller who makes data available to third parties for use in their direct marketing activities.

"data user" is an organisation making use of either its own data or of data obtained from other sources for any direct marketing purpose.

"list" or **"database"** means personal information held for direct marketing purposes that is normally accessed by reference to names and addresses and is held in the form of a paper or electronic list.

"the Data Protection Principles" are the eight enforceable rules contained in the Data Protection Act 1998 which prescribe the required conduct for the lawful management of personal data.

"unsolicited commercial communication" is a communication sent to consumers with whom the sender does not have an ongoing commercial or contractual relationship or where such a communication is otherwise uninvited.



"the European Economic Area" is the twenty-five member states of the European Union plus Norway, Iceland and Liechtenstein.

"Information Commissioner"

These two terms are used throughout the publication, however they refer to the same thing.

The terms **"customer"**, **"respondent"**, **"recipient"** and **"participant"** refer to people, whether they are receiving direct marketing in their private capacities or in the course of their employment.

"Prospect" Person who may become a customer

"Warm Prospect" A person with whom a relationship has been established

"Cold Prospect" A person with whom no relationship has yet been established



SECTION A

Why Best Practice?

The use of data is key to most direct marketing activities. Whether the campaign is a simple list selection and mailing, or utilises complex databases and processes to arrive at a targeted audience, adoption of best practice in use of data has an equal importance.

The dynamics of today's marketplace means that data held about the individual begins to decay as soon as it is gathered.

For example:

- approximately 13% of the UK population move house each year Office of Population Censuses & Surveys (OPCS);
- approximately 11% of addresses are mailed incorrectly each year Direct Mail Information Service (DMIS);
- 45% of the UK population believe that a mis-spelt name or address is an indication of 'junk mail' Direct Mail Information Service (DMIS);
- 1.1 million UK households (as of October 2003) are registered with the Mailing Preference Service (MPS). For further information see section I

In most direct mail campaigns the list (or file) of target prospects or customers may undergo a journey between a number of organisations involved in different parts of the production process e.g. list owner, broker, computer bureau, laser printer, mailing house, etc.

It is therefore vital that during all these processes, accuracy, integrity and security of the data is maintained to the highest standards (please refer to Section E: Receipt and Transfer of Data).

The benefits of best practice in use of data are quite clear:

- helps direct marketing become more cost effective, avoids waste for the advertiser and saves money;
- reduces potential annoyance to recipients through duplicated mailing, incorrect or mis-spelt names and addresses;
- helps advertisers target mail more effectively, enhancing the advertiser's image with his customers and prospects;
- well targeted and produced mail provides a more confident message to consumers about direct marketing and DMA members;
- best practice is an important part of industry self-regulation.

This guide also covers areas of data usage which are included within the DMA Code of Practice or by specific legislation. The Data Protection Act 1998 is the principal legal framework within which all personal data may be handled. These guidelines set out where responsibility lies between clients and bureaux for ensuring compliance with the Act at each stage of data usage.



The outcome of following the best practice guidelines should be better performing communications which build customer relationships and long term loyalty. These are objectives which the whole industry shares and which the Data Council and the DMA endorse.



SECTION B

Data Protection and Related Legislation

Whether using customer or prospect files, in business-to-business or consumer markets, it is important to remember that commercial access to data is a privilege, not a right.

Except for public domain information, every item of data used has been given freely and voluntarily by the data subject, with the expectation that it will be used fairly, appropriately and legally.

The Data Protection Act 1998 came into effect in March 2000 and implemented the 1995 European Data Protection Directive. Companies, which complied with the 1984 Data Protection Act's eight principles should experience few problems in complying with the new legislation, although there are some important changes.

To maintain best practice in the use of data, marketers should also have in place facilities to ensure that data is as up-to-date as possible and that all suppressions are respected. A change of address file, either proprietary or commercial, should be used to validate addresses before they are mailed.

Notifications of changes to details, such as address, telephone number, job function, etc, should be recorded and added to the master file within a reasonable period of time. Requests not to be mailed, phoned, faxed, emailed or texted (separate from Mailing, Telephone and Fax Preference Service registration) should be logged on 'Do not mail', 'Do not telephone' 'Do not fax' 'Do not email', or 'Do not text lists' and used as a screen before carrying out any communication. For more information on: Email, please refer to the Email Marketing Best Practice Guidelines
SMS, please refer to the Contact Centre Guidelines
Privacy and Electronic Communications (EC Directive) Regulations 2003, [click here](#).

The client is responsible for ensuring that:

they are registered as a data controller,

- where processing of personal data is carried out by a bureau on behalf of a client, the client should in order to comply with the seventh principle of the Data Protection Act 1998:

a) choose a processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and;

b) take reasonable steps to ensure compliance with those measures.

- where processing of personal data is carried out by a bureau on behalf of a client, the client is not to be regarded as complying with the seventh principle of the Data Protection Act 1998 unless:

a) the processing is carried out under contract:

i) which is made or evidenced in writing, and;

ii) under which the bureau is to act only on instructions from the data controller, and;

(Please [click here](#) for a link to the suggested DMA data processing contract and guidelines)



b) the contract requires the bureau to comply with obligations equivalent to those imposed on the client by the seventh principle.

- any in-house database and use of personal information is correctly registered;
- all data has been acquired and processed in accordance with the Data Protection Act 1998;
- any marketing communication using personal data complies with the British Code of Advertising and Sales Promotion (the CAP code);
- facilities are in place for updating data, registering requests not to be mailed or phoned, or to permit access to data by its subject;
- third-party data rented from a commercial data owner in membership of the DMA is supported by a list owner warranty.

The supplier is responsible for ensuring that:

- the data controller is fully and correctly registered with the Data Protection Commissioner (all current notification details are now accessible online at <http://forms.informationcommissioner.gov.uk/search.html>);
- data is held and used in accordance with the Data Protection Act 1998 including notification of its business and security of the data;
- lists are screened against the most recent version of Mailing Preference Service (MPS), Telephone Preference Service (TPS) or Fax Preference Service (FPS) and consideration of other screening files is taken;
- any communication using data which they own/manage complies with British Code of Advertising and Sales Promotion (the CAP code);
- requests to be removed from a list, to have details corrected, or to have access to the information held are properly dealt with;
- list owners hold a list owner warranty, where appropriate.
- prompt action should be taken to respond to a customer request in writing for access to his or her personal data. Under data protection legislation, all information held has to be provided promptly and in any event within a maximum of 40 days, subject, if thought appropriate, to a fee with a current maximum of £10. Such requests should be dealt with as a customer service in a spirit of transparency and good faith.



SECTION C

Caring for Personal Data

Particular care should be taken when handling, processing and using files containing personal data. Customer data is particularly valuable. One of the principal drivers of direct marketing is to retain existing customers. It is estimated that it costs one-fifth the amount to sell to an existing customer as it does to make a new sale. During the course of a customer's lifetime, it is also likely that a greater wealth of data will be generated and more sensitive items, such as date of birth or financial status, may be held. To retain customer and therefore prospect customer's trust, all personal data must be processed with care.

The DMA recommends that the following points are given special consideration when dealing with all personal data:

- particular care should be given to the data capture process, the first principle of the Data Protection Act 1998 (see also Schedule 1 Part 2 and Schedule 2) especially where the information being captured may be sensitive personal data under the Data Protection Act 1998 and for which special rules apply (see Schedule 3 of the 1998 Act);
- the fourth principle of the Data Protection Act 1998 should underpin the management of personal data. This states that, "personal data shall be accurate and, where necessary, kept up to date." The data owner should be conscious of the time sensitivity of data and the fact that it will age over time;
- an appropriate updating cycle should be implemented to ensure that the data held is accurate and up to date. Immediately prior to a communications programme, extra emphasis should be placed on refreshing customer data;
- 'address' management procedures should be in place to maintain the accuracy of customer addresses. These should include: updating of the postal address using software which references the Royal Mail's Postcode Address File (PAF); using customer notifications of change of address, or employing proprietary change of address or suppression files. These processes can be carried out in house or through a DMA member bureau;
- the seventh principle of the Data Protection Act 1998 states that data must be kept secure. Your business procedures should ensure that no customer or prospects listings are left lying around or discarded in waste bins which could ultimately end up on a public tip, that computer screen on which personal data is displayed are not visible to unauthorised personnel and that when handling enquiries by phone which may result in personal data being discussed or revealed that the identity of the person at the end of the phone is verified.

Section I covers the process of screening data files to remove or suppress records as appropriate. Reference is made to screening files which must be used by law as well as those that should be used as best practice.

For email please refer to the DMA Email Marketing Best Practice Guidelines



Section D

Data Capture

To make use of data – whether name, address, telephone number or any other element the information has to be captured at some point. Achieving the highest level of accuracy and consistency at this stage will reduce problems with data processing and use later, as well as improving results from any analysis or contact made using the data. Three key sources exist from which data may be captured – print (mailed/faxed response), telephone or electronic media.

Coupon response

When designing a marketing communication which will generate a physical response in the form of a coupon, consideration should be given as to how data capture will be facilitated. Whether cut from a press ad, mailshot, catalogue, leaflet or other printed material, the coupon should prompt the consumer to provide data that is both sufficient and accurate. To support good quality data capture, a coupon should:

- provide sufficient space for all the data elements required. The average UK name and address record is 48 keystrokes long, but it can involve up to nine separate lines of information. While use of data for postal purposes may only require the delivery point and postcode, consumers have preferred address elements such as a house name. Business addresses can be even longer and business titles more varied still;
- prompt the respondent for key data elements. Separate lines or boxes for title, initial or name, address and postcode will improve the quality and accuracy of data compared to free form text boxes. A specific prompt for postcode and house number will improve speed and accuracy.
- include a separate prompt for country if data is being gathered from multiple countries. This precludes the need for subsequent assignation of each response to a country of origin;
- allow variations in handwriting, ink colour, etc. Using blocks or 'tiger teeth' to denominate spacing for characters can be a useful way to improve legibility. This may also allow coupons to be data captured using faster optical character recognition (OCR) processes. Coupons should not be printed on strong colours (i.e. reversed out of black) or over images as this will make completion and reading harder;
- be tested before signing off on a campaign by asking a friend or colleague to complete it.

Telephone response

An increasing volume of response is being generated via the telephone. This gives an ideal opportunity for data capture of both name and address as well as other information, subject to time and cost constraints and relevant legislative guidelines.

To support best practice in data capture, telephone response mechanisms should:

- allow the respondent to provide information at his or her own speed where automate call handling/interactive voice response (ACH/IVR) is being used. The system should prompt for name and address elements, including a double check for key elements, such as postcode. A prompt to spell difficult words should be included to facilitate transcription unless these are covered by reference to PAF;



- include an initial request for the caller's postcode in live operator scripts. Computer software can return the correct postal address from this, allowing operators to validate it with the caller and add the house number and any preferred address elements. This will also reduce the duration of calls;
- avoid open-ended questions, as these extend call times. Data capture requests should be restricted to yes/no categories, banded information (such as age in ten year steps), or multi-choice prompted responses.

For more information:

Link to Privacy and Electronic Communications (EC Directive) Regulations 2003(c), [click here](#).

Fax Marketing

Fax marketing is increasingly being used as part of the marketing mix and this gives rise to a number of issues from a data capture point of view.

To support best practice in data capture, fax marketing mechanisms should:

- ensure that adequate arrangements are in place to receive and record details of recipients who do not wish to receive further fax mailings, whether such requests are made by telephone, fax or mail. Any such telephone requests should be dealt with sympathetically and sensitively by the issuing organisation;
- ensure that the fax number of such 'do not fax' recipients are removed from the respective fax lists in a timely manner after notification and not called in future campaigns;
- ensure that any consumers, or businesses operating from a consumer premise, are made aware of the FPS contact number if they indicate a more general 'do not fax' requirement beyond the actual fax marketing piece in question;
- ensure that any delivery report information following a fax mailing is diligently used in a timely manner to maintain up to date fax lists for future use.

Electronic media

(For further information, please refer to the DMA Email Marketing Best Practice Guidelines)

Growing use of the Internet and email will allow highly personalised communications, based on detailed information about targets. Care is necessary at this stage, however, due to the distinctive culture of these media.

Online data capture mechanisms should:

- respect the prevailing 'netiquette'. Many users of the Internet object to commercial communications which they have not requested;
- use online address validation software to check the address details entered and confirm with the user any questionable details. Remember that an email address does not give any indication of where a user lives, or their age so prompt for country of origin and date of birth;



- make access to higher levels of an online site conditional on the provision of personal data, but do give some value to users who do not wish to leave their details;
- DMA members should comply with the relevant online sections in the DMA Code of Practice.

For more information:

Privacy and Electronic Communications (EC Directive) Regulations 2003, [click here](#).

Using data capture bureau

Data capture involves two elements. The initial stage is the conversion of coupon or telephone responses into an electronic file via optical scanning, re-keying or transcription. This produces a list which is identical to the responses received, with information exactly as provided by respondents. In the second stage, this data may be validated, enhanced or corrected.

Choosing a data capture bureau requires decisions to be made about the level of accuracy required and the extent of further work required on a file. Best practice guidelines include:

- selecting a bureau with relevant experience and expertise. Data capture may be carried out from market research surveys, postal lifestyle questionnaires, coupon responses, etc. Each of these employs a different skills set (and possibly different technologies). Ensure the supplier has the appropriate knowledge;
- many suppliers of data capture are based offshore. This can offer significant savings, even when allowing for freight costs. Members need to be aware of the eighth principle of the 1998 Data Protection Act. To comply with the law, data will be allowed to be exported only to countries outside the European Economic Area, which have an adequate level of data protection. Members should not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for data subjects, or where an alternative means of ensuring adequacy exists such as through an appropriate contract. Members are strongly advised to consult the DMA's Legal Department or their own legal adviser's on this point.
- selecting a bureau which offers the necessary facilities if data needs to be validated or enhanced. Data quality will be improved if a supplier has the appropriate services, such as default character setting, range checks on numeric data, address validation procedures, data enhancement and telematching;
- agreeing the format and schedule for data output in advance. Responses may be sent for data capture and returned in batches, or as a single consolidated set. If frequent, regular data transfers are required, it is advisable to use a bureau with electronic transfer facilities;
- obtaining signed, written agreements in advance of any work being undertaken. In addition to standard contractual obligations, these should also cover liability for data and confidentiality;
- ensuring that plans have been made for retrieval of original documentation. This may be a legal requirement for some product categories, in case a dispute or query



arises. Documents may be converted into digital or optical files for faster retrieval and ease of storage. Ensure that correct procedures have been agreed for the disposal of all original documents, including incineration or shredding as appropriate.

Benchmark

The level of accuracy for data capture should be agreed in advance between client and bureaux. This should be defined for each job undertaken and is usually expressed in percentage terms, for example, % rejects and % invalid addresses. Request and check a test file to ensure these levels are being met. A 1 in N or random sample of the final file may also be checked.

Where data is to be validated and enhanced, agree separate rates of accuracy for matching to address verification files. The type of verification and definition of a match should also be specified.

The client is responsible for ensuring that:

- methods of data collection are designed to maximise accuracy, legibility/audibility and completeness of information supplied by respondents;
- suppliers comply with data protection laws, as appropriate;
- specifications for data capture are supplied, stating levels of accuracy and matching required;
- procedures are in place for retrieval or destruction of original documents after data capture.

The supplier is responsible for ensuring that:

- work is only accepted for which it has the appropriate skills and technology;
- up-to-date verification tables are maintained;
- data and documents are processed and stored securely, in line with the Data Protection Act, and are returned or disposed of according to the client's brief once work is complete.



SECTION E

Receipt and Transfer of Data

The transfer of data files is a basic, but critical process. A single project may involve the sourcing and transfer of hundreds of separate files, with a delivery schedule covering several weeks. Managing and controlling this process is critical to the orderly handling of data.

All transfers, handling and storage of data should comply with the Data Protection Act 1998. Data owners are responsible for checking the security arrangements operated by any third party to which they transfer files. Data owners should ensure data will be held securely and files processed lawfully.

Every data owner will have a preferred file format. Where data is sourced from multiple owners, both from the client's in-house database and from third parties, this means the bureau will have to convert each file into a common format for processing.

Documentation of each file layout needs to be supplied to allow the bureau to prepare conversion procedures. Each file then needs to be notified to the bureau by the client, and logged on receipt. Accurate management of files in this way will allow cross-checking of planned data use with actual use. On receipt, the bureau should confirm the file layout, size, readability, and status against the client's data schedule. All files should be stored in a secure environment.

The bureau should be capable of handling data in most common media formats, including DAT, diskette, magnetic tape, cartridge, CD and electronic data transfer. Notification should be given by the client of the format in which each file will be delivered, together with any unusual media to be used. Resupply of data will be necessary if a file does not tally with the documentation, or if it is corrupted. Electronic data transfer requires particular care because of the increased possibility of data being corrupted during transmission. Documentation should be supplied either as part of the file transferred, or separately on paper.

Members should take appropriate technical and organisational measures to ensure that personal data is held securely and safeguarded against unauthorised use, disclosure or alteration and accidental loss, damage or destruction.

Once processing has been completed, the data should be returned by the bureau to its owner. Industry practice is for the original data files to be returned exactly as supplied. Records on all data transfers should be maintained to allow for an audit trail once the process is complete, if required.

The client is responsible for ensuring that:

- a schedule of files to be used is supplied in advance;
- notification of media to be used, including uncommon formats, is provided;
- use of data complies with the Data Protection Act 1998 and is held, disclosed and processed lawfully;
- full documentation is provided for each file, covering project reference, file layout, supplier contact details, sample print, number of records and return instructions;



- test files are supplied when requested by the bureau;
- delivery schedules are met, unless previously notified;
- reasonable steps are taken to ensure that files supplied are virus free.

Ensuring that the supplier has a proven and robust disaster recovery plan sufficient to protect their data and the project. Consideration should be given to the nature and value of the project being undertaken by the supplier on behalf of the client.

The supplier is responsible for ensuring that:

- all files received are checked against the client's schedule and examined for readability and size;
- any discrepancies or problems are notified to the client promptly;
- all data is processed and stored according to the Data Protection Act 1998;
- incoming data is checked for viruses and data owners are informed immediately of any problems;
- the schedule for processing is followed as agreed, subject to prior notification of any changes or delays;
- each file is given a unique identification to allow it to be reconstituted at the end of the project and tracked through processing;
- data is returned to the client/data owner at the end of the project in its original format, subject to prior agreement;
- the supplier should also consider whether the bureau should have professional indemnity insurance to cover the bureau's liability for loss, damage or theft of data whilst held and processed by the bureau. [Click here](#) to download a draft data processing contract.



SECTION F

Name and Address Cleaning

In order to carry out effective record matching for the purposes of deduplication, screening and data enhancement and also to get the best possible postal discounts for mailings, it is essential to carry out name and address cleaning. This is a critical foundation for Customer Relationship management and the ability to create a 'single customer view'.

Different data suppliers, whether they are commercial list providers or clients, will hold name and address data in a format specific to their internal processing requirements. The quality of the data in terms of accuracy and completeness of the information may also vary considerably depending on its origins.

The process of 'converting' or 'reformatting' the data involves making sure that the data across multiple sources is in a consistent format that can be processed by bureau or in-house software i.e. postcodes in the same fields.

The process of cleaning involves making sure that the accuracy of the name and address data is as good as possible as detailed below:

Name Processing

A good bureau will usually 'hold a number of reference tables to assist with processing names. These are likely to include:

- Standard abbreviations for titles
- Correct decoration suffixes
- Forename variants
- Salacious and 'nonsense' names

Care should always be taken when making any changes to names due to the sensitivity of this information and the difficulty of holding information on all possible names and variations.

A good bureau should also be able to append the correct salutation based on name and title. It should also be possible to apply a default salutation where an accurate salutation is not possible because of ambiguous name information where no title is present e.g. Chris Jones. Default salutations include such options as Dear Customer, Dear Occupier etc

Examples:

Data in: Mjr John Filmer mbe
Salutation: Dear Major Filmer
Envelope: Major John Filmer MBE

Data in: Avm Jack Jones Mbe
Salutation: Dear Air Marshal Jones



Envelope: AVM J Jones MBE

Data in: Sir John Smith
Salutation: Dear Sir John
Envelope: Sir John Smith

Address Processing

The main external reference table used by most bureaux as the basis for checking and correcting addresses is Royal Mail's Postcode Address File (PAF). PAF contains all known addresses and postcodes in the UK including England, Scotland, Wales, Northern Ireland, Jersey Guernsey and the Isle of Man (over 26 million addresses 1.71 million postcodes).

PAF will often be incorporated into general address cleaning software but will normally be the benchmark against which addresses are checked and corrected. However bureaux should also have the flexibility to incorporate client business rules if required. These may include some of the following:

- Customer preferred addresses (sometimes known as vanity addresses or cherished addresses) where elements of the address are not the address recognised by Royal Mail and therefore not how the address may be held on PAF

Examples:

The Old Stables	29 Burnham Road
29 Burnham Road	Tunbridge Wells
Tunbridge Wells	Kent
Kent	TN12 4ZP
TN12 4ZP	

10 Vicarage Road	10 Vicarage Road
Battersea	London
London	SW11 2LY
SW11 2LY	

- Retaining the input address – an example of this may be where the data is billing data

Updates to PAF are made on an ongoing basis by Royal Mail to accommodate new buildings or to improve delivery efficiency. These updates are available to bureau and clients in a number of different formats and frequencies (monthly updates are the most frequent) and bureaux should adopt these changes within a reasonable amount of time. A good benchmark is that they are adopted within 3 months of the changes being made.

Companies will usually also have the ability to correct inaccuracies in addresses to improve the chances of them matching to PAF. Different bureaux will have different capabilities depending on their software however the following are likely to be included.

- Matching old postal geography to new



Examples:

NEWPORT, MON becomes NEWPORT, GWENT.

NEW MILLS, STOCKPORT, CHESHIRE becomes NEW MILLS, HIGH PEAK, DERBYSHIRE.

SANDHURST, CAMBERLEY, SURREY becomes SANDHURST, BERKSHIRE.

- Correcting common misspellings, omissions and transpositions

Examples:

BIMRINGHAM becomes BIRMINGHAM.

CRODON becomes CROYDON.

MANNCHESTER becomes MANCHESTER.

GUISELEY LS20 8HU becomes GUISELEY LEEDS LS20 8HU.

- Recognising common edit marks

Examples

STOKE ON TRENT and STOKE-ON-TRENT.

SOUTHEND/SEA & SOUTHEND ON SEA.

- Correcting common abbreviations and superfluous words

Examples

BRUM for BIRMINGHAM,

HANTS for HAMPSHIRE,

MIDDX for MIDDLESEX.

Business Data

The principle activities involved in processing business data are the same as in processing consumer data i.e. checking and correction of names and addresses by reference to PAF and other tables.

However there are added complexities with business data because of the additional information contained in a business record including the following:

- Records may be contact names at a company with an address or just a company at an address e.g. Fred Smith, Bloggs and Co, 1 The High Street, Maidstone ME15 1SA OR Bloggs and Co, 1 The High Street, Maidstone ME15 1SA
- Records may also contain Job Title and Department information e.g. Fred Smith, Tester, Manufacturing Department, Bloggs and Co, 1 The High Street, Maidstone ME15 1SA



In addition, the following points should be considered:

- Setting business rules governing whether the Company Name as it appears on PAF should replace the input name
- Consult closely with your bureau on processing business data

Overseas data

Requires specialist processing to incorporate non-UK postal address information. However bureaux should have the capability to recognise non-UK records within a data file and side file. Many UK Bureaux are able to provide address management. Ask your bureau for details

The client is responsible for ensuring that:

- The supplier is advised of the nature of the data to be processed i.e. whether the data is business or consumer data and whether it contains any non-UK records. If possible it is useful to supply a sample of data in advance so the bureau can check for any likely problems
- A file layout is supplied for the data with separate layouts being provided for different files where required
- Any client specific business rules are clearly set out and understood

The supplier is responsible for ensuring that:

- External and internal verification tables, such as PAF and Royal Mail postcode changes, are accurate and up to date
- Any problems with the data received are advised to the client as soon as possible
- A clear brief has been received and understood and any special processing requirements have been clarified and agreed
- Audit reports are provided showing the progress of records through the process including how many records have been dropped and why
- Any queries are raised with the client as soon as possible



SECTION G

Name and Address Matching

Matching name and address records is carried out for three key purposes:

1. to identify and/or remove duplicate records from a file. Lists and databases often contain internal duplicates, usually where the same individual has been recorded twice, or where the same individual has provided details in different formats. Matching these and suppressing them reduces wastage and improves the performance of a file;
2. to screen a file against other data sources for validation or suppression. The file may be matched against external data sources, such as the edited version of the Electoral Register, county court judgments, deceased or gone-away files. This process ensures that a communication is made only to individuals who have been verified to be at an address, or to be in the appropriate target group. Matching against the TPS or FPS file is required by legislation, where a communication is unsolicited matching against MPS, is required under the DMA's Code of Practice;
3. to enhance, or 'tag', additional data to a file. Additional data, such as date of birth, telephone number, or lifestyle characteristics, may also be added to a file from a matched external data source. This will help to improve targeting and may also be used when planning communications. In each case, a decision will need to be made about the level of accuracy to be tolerated in matching. Each bureau will use a different technique. Consequently, different suppliers will achieve different levels of matching. It is important to understand how the technique used affects this accuracy and whether matches are in fact real. All software will also produce a certain error rate – the tolerance of this should be agreed in advance between the client and the bureau.

Example:

In order to achieve correct matching, bureaux need to be able to identify ambiguous addresses and offer alternatives. Typical difficulties arise out of mis-spelt addresses that could be resolved into either of two places. Boston, Lincs and Bolton, Lancs are commonly confused.

INCOMING ADDRESS: MATCH ONE: MATCH TWO:
2 Church Road 2 Church Road 2 Church Road
Bolton Farnworth BOSTON
Lincs BOLTON Lincolnshire
BL4 8AL PE21 0LW

Where data is to be suppressed or enhanced, there are risks associated with matching. Removing a record which appears to be a duplicate, but which in fact is just very similar, such as identical surnames in the same households, could lead to a customer failing to receive information to which he or she is entitled. For this reason, financial services clients will often accept a lower level of match rate, for example. Equally, appending data to the wrong record might lead to inappropriate targeting of communications. A higher match rate could be called for in these circumstances.

Matching Levels

Where no data is to be overlaid, matching and deduplicating a file is usually carried
DMA Data Best Practice Guidelines. © 2004



out with a level of overkill – suppressing even doubtful duplicates in order to reduce wastage. Underkill is more appropriate where a data overlay is to be applied. This not only avoids the risk of incorrect targeting as noted above, it will also minimise the cost to the client of licensing this data.

As a rule, matching software should not be dependent on a single data element. This will avoid the suppression of a file as a result of a spelling error in the source file. A hierarchy should be agreed which weights each data element to be used in the match. For example, the postcode is a strong matching point, but should not be used in isolation since a single character difference could result in a failure to match. The second initial in a name is a weak matching point and may be overlooked where it differs, if all other elements are the same.

Consumer record matching

Consumer file matching can be undertaken at a number of different levels:

1. matched on title, initials/forename, surname and address;
2. matched on surname only and address;
3. matched on address only.

A single data processing project may require matching at more than one level. For example, when screening against a deceased file, the match is commonly undertaken at the surname and address level. Matching rented lists against each other might be at the finer, full name and address level.

The impact of each level should be clearly understood. Where address only matching is used, if multiple occupiers with different surnames are present at one address, only one of those records will be retained, for example.

Business record matching

Business file matching can be undertaken at a number of different levels

1. matched on title, initials/forename, surname, company and address;
2. matched on company and address;
3. matched on address only.

Job titles and departments add a further degree of complexity to business data matching. For example, two records could share exactly the same individual and company name, but have a different job title – these may or may not be the same person.

Another difficulty is the ability to identify accurately all the supplied data elements. Both company names and job titles are often abbreviated and presented differently across files. The bureau should hold tables which are able to identify these as matches, for example, recognising International Business Machines and IBM as the same company.

Matching at a “coarse” level will have an impact on the final file size. For example, using address only will result in only one record being retained in a match where multiple companies share the same address.

Non-name and address matching



Another option available in a deduplication process is the use of non-name and address data. During a data tagging project where precise matching is important, the use of personal data such as date of birth or bank account number is a useful means of ensuring records to be merged are definite duplicates. The data element chosen will also have to be one which has a high level of population on the files being matched.

Best practice for postcodes is to be able to identify and select as follows:

- accurate;
- confirmed to thoroughfare level;
- confirmed to dependent locality level;
- confirmed to post town level;
- missing or unverifiable.

The client is responsible for ensuring that:

- a clear and written brief is provided for the type and level of matching to be used;
- the acceptable degree of tolerance within each of the matching levels to be used is stated;
- further information requested by the supplier is supplied in a timely fashion;
- where a data audit (i.e., sample of file with verification of matching) has been requested, this is signed off promptly.



SECTION H

Deduplication / Merge-Purge

Where a variety of data sources are being merged to produce a single mailing list or phoning file or to populate a database, deduplication i.e. the removal of records which occur more than once when all data source are combined, is an essential step in the overall data preparation process.

The actual process of deduplication includes the identification of records which are considered to be the same and the selection of one of those records to be used / retained. The process is also referred to as merge-purge.

To carry out the deduplication process, a hierarchy of the data sources being used must be constructed. This means that where a duplicate is found, the record on the list with the higher preference is used, while those on the list(s) of lower preference are discarded. In relation to mailing and telephony files deduplication may have a significant impact on data costs, since under net name deals, only those records used will be paid for. How the hierarchy is constructed and used will depend on the overall objective for the marketing campaign (or database population) and the budget available.

The most common deduplication options are:-

Random: All data sources are viewed as equally valuable. This option is commonly used when there is no experience of the data sources being used, or in testing.

Cheapest Lists First: This provides a file with the lowest list cost (where net names rebates are all similar). This is useful where the client has no experience of the list.

Lowest Nets First: Those lists for which the client has agreed the lowest net name rebates are placed first.

Cheapest Cost Per: This produces the most cost effective list. This is only possible Response First where the client has previous experience of the list. Some industry sectors require special care. For instance, financial services companies often have joint customers. This produces single records, which may contain more than one individual name sharing an address. Deduplication against one of these files will require additional care to ensure that both the joint names can be used to match and suppress any duplicate.

Duplicate identification

The deduplication process can usually be set to identify duplicates / select records at different levels within the data. In consumer data for example you may opt for:

- 1 per person
- 1 per address
- 1 per household (or surname at address)

In business to business data additional element can be added e.g.

- 1 per job title
- 1 per department



It is essential to understand the actual composition of your data file when setting your deduplication options. For example choosing to select 1 per job title when only 25% of the records on the file contains job titles is a non starter!

Many clients recognise that they require different standards of deduplication depending on the information that they have about individuals. For instance, clients may wish to take greater care not to send a duplicate mailing to an existing customer than they require for simple prospect mailings. In that case, they may define a duplicate as anyone sharing a postal address with a customer or, where there is no customer presence, individuals sharing a surname and address.

Net name rebates are affected by where in a hierarchy the list is introduced for deduplication. The later in the process, the higher the number of duplicates that will be produced. To maintain trust in this process and in negotiation with list suppliers, the bureau must maintain and provide to clients complete audit trails. Reports on the validity of duplicates, in the form of samples of duplicates and of the deduplicated file, must also be supplied.

The client is responsible for ensuring that:

- a clear and written brief is supplied of the required definition of a duplicate, the hierarchy of list preferences, and any non-standard processing that is required;
- external data sources to be used for deduplication are supplied on schedule;
- agreements with data owners on net names are complied with in the hierarchy constructed.

The supplier is responsible for ensuring that:

- the client understands fully the types of duplicates which can be identified
- an accurate and complete audit report is provided showing the numbers of duplicates identified and their distribution across list sources;
- all counts provided will be auditable by printing the corresponding addresses, if required;
- processing is carried out in the order agreed with the client and in a timely manner.



SECTION I

Screening / Suppression

Screening is the process of checking the names on your list or database against another list or database specifically built for that purpose and removing / suppressing (or screening out) those which match. Use of these screening files typically incurs costs in two areas (a) processing and (b) for the number of records suppressed.

Data used for screening generally falls into three categories:

Client specific

Data that the client has collected on individuals with whom it has traded previously is a highly discriminating screen. It includes files on:

- existing customers and prospects;
- individuals with whom the client has a previous bad trading experience;
- individuals who have requested not to be mailed, faxed or phoned.

Sector specific

Data that has been built within an industry sector may be pooled by companies operating in that sector for sharing. The two best known are files on:

- individuals with a poor credit record;
- individuals who have made insurance claims.

Generic data

Address based files are often used for screening. The most widely used include files on:

- individuals who have registered with the Mailing, Telephone and Fax Preference Services (MPS, TPS and FPS respectively);
- individuals who are known to have died ('deceased');
- individuals confirmed to have moved ('movers');

Follow this link (add link) to the DMA's Top Tips on Suppression document.

Guidelines

MPS: DMA members must ensure that no list containing consumers is used for prospect mailing purposes unless it has been cleaned against the Mailing Preference Service (MPS) file. Members must ensure that such a list is cleaned against the most recent MPS file no more than 90 days before supply, although a user may choose to clean it again before use. Members may use their own list (i.e. a list of those with whom they have an established relationship) without cleaning against the MPS file.



TPS: Members must ensure that no list containing individuals(and corporate numbers with effect from 23 July 2004) is used for telephone marketing purposes unless it has been screened against the Telephone Preference Service (TPS) file. Members must ensure that such a list is cleaned against the most recent TPS file no more than 28 days before supply, although a user may choose to clean it again before use. Members may use their own list (i.e. a list of those with whom they have an established relationship) without cleaning against the TPS file, as long as the data subject has provided their telephone number (i.e. it is not sourced) and it is made absolutely clear at the time of collecting the telephone number that the data subject may receive telemarketing calls to that number.

FPS: Members must ensure that no list is used to send unsolicited fax marketing messages to businesses unless it has been cleaned against the Fax Preference Service (FPS) file. Members must ensure that such a list is cleaned against the most recent FPS file no more than 28 days before supply, although a user may choose to clean it again before use. Members may use their own list (i.e. a list of those with whom they have an established relationship) without cleaning against the FPS file, as long as the data subject has provided their fax number and it is made absolutely clear at the time of collecting the number that fax marketing numbers may be sent to that number.

Use of the TPS and FPS files is a statutory requirement.

Failure to screen against the TPS, FPS or an in-house 'do not contact' list will have legal consequences.

BMPS: Members must also ensure that no list containing consumers, including a list of those with whom they have an established relationship, is used for baby related mailings unless it has been cleaned against the Baby Mailing Preference Service (BMPS) file. The BMPS file gives bereaved parents the option to have baby/infant related mailings suppressed for 12 months.

The client is responsible for ensuring that:

- a clear and written brief is provided of the screening process to be used and the level of screen to be used;
- external data sources to be used for screening are supplied to the bureau in a timely manner.

The supplier is responsible for ensuring that:

- screening is carried out in accordance with the clients' brief and schedule;
- an accurate and complete audit report of the entire process is provided showing the numbers of individuals screened providing balanced professional advice on all suppression / validation / enhancement.



SECTION J

Data Tagging and Enhancement

Data tagging is the addition of extra data to the client's database from external sources. The purpose of data tagging is two fold:

- to improve the data used in targeting, especially if statistical modelling is used for selection;
- to generate a more individual message within the mailing (for example, a sales message that relates to the individual's date of birth).

The sources most often used for the external data are:

- the edited version of the Electoral Roll can be used;
- lifestyle databases;
- pooled databases of clients' trading data.

The advantages of data tagging can be substantial. However, the costs of tagging are usually considerable. To be cost effective, it is likely that only selected segments of a customer file will undergo data tagging.

There are also considerable risks involved. For example, if the tagged data is not used correctly, customer annoyance may outweigh any marketing benefits. This may occur if:

- data has been incorrectly captured or is inaccurate;
- data has been incorrectly matched;
- data is incomplete.

The first of these two risks can be mitigated by careful matching. Matching procedures need to ensure that there is minimal possibility that two individuals within a household or company may be confused. Matching at surname and initial may not be sufficient if there is any likelihood that there will be two individuals with the same surname and initial within the household or company. Ideally, a match will be made using additional data, such as date of birth or job title.

The problem of incompleteness – not being able to tag data for all individuals on a file: applies mainly where the data is being used for the creative message. This could compromise the creative treatment if it relies on the missing data element being inserted into the message.

Statistical and modelling tools exist which can predict what the missing data should be. These can be used with varying levels of confidence, depending on the level of records for which that data element is present. Segmentation and selection tools will have procedures for handling data sets with missing data elements. Predictive data is not used for definitive client specific messages.



The client is responsible for ensuring that:

- a clear and written brief is provided on the type and level of data to be tagged;
- any external data source from which data is to be tagged is supplied in a timely manner;
- tagging levels are agreed and a sample of matched records is signed off.

The supplier is responsible for ensuring that:

- the client is advised on the tagging options and their implications;
- tagging is carried out in a timely fashion and to the agreed specification;
- tagged files and external data sources are returned promptly and in good order;



Section K

(For more information, please refer to the Royal Mail website: www.royalmail.co.uk)

Sortation and Output

1. Sortation for Postal Discount Schemes

Data can be sorted into any sequence requested by a client however it will be sorted in a sequence that will facilitate bulk mailing discounts from Royal Mail. There are a number of Royal Mail discount schemes, including Mailsort, Walksort and Cleanmail plus parcel discounts for catalogue mailers including Presstream.

The schemes generally provide postage discounts in return for minimising the amount of preparation and sortation work Royal Mail are required to do themselves. This is based on levels of accuracy of postcoding together with the volume of items being mailed at any one time.

Example:

Mailsort 1400 requires a minimum mailing of 4,000 items and 90% of the file should be accurately postcoded. Depending on further selections within this service, discounts can be anywhere between 8% and 30%.

A good bureau should be able to process data to meet the requirements for each of the schemes including the required levels of postcoding plus the production of all the required support documentation.

The full details of the schemes are contained on Royal Mail's web site [Royal Mail's information and services portal](#)

2. Mail File Segmentation

When carrying out a mailing it is likely that there will be different packs and messages for different segments of the target audience including a control cell. A good bureau should be able to segment the final mailing file based on the client's selection criteria and output this to the mailing house or printers.

3. Output Media

A good Bureau should be able to output data in various formats and using different media types e.g. FTP, CD etc. It is important that early consideration is given to the final output required and that this is discussed with both the Bureau and Mailing House or Printer. A supply of test data to the printer is important to allow sign off on a sample of print.



Appendix – Useful addresses

DMA (UK) Ltd

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7321 3300
F 020 7321 4165
E dma@dma.org.uk
W www.dma.org.uk

DMA North

c/o Karen Millett Marketing Consultancy
25 Stradbroke Avenue
St George Bristol
BS5 8PJ
T 0117 935 2908
E karen@dma.org.uk
W www.dma.org.uk

DMA West

West Wing
Arle Court
Cheltenham
Gloucestershire
GL51 6PN
T 01242 545 325
E andrew@dma.org.uk
W www.dma.org.uk

DMA Edinburgh

41 Comely Bank
EDINBURGH, EH4 1AF
T (0131) 315 4422
F (0131) 315 4433
E jo@dma.org.uk
W www.dma.org.uk

Information Commissioner

Wycliffe House
Water Lane, Wilmslow
Cheshire, SK9 5AF
T (01625) 545745 enquiries
(01625) 545740 registration
W www.informationcommissioner.gov.uk

Preference Services: Mailing, Fax, Telephone, Email, Baby

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7321 3300
F 020 7321 4165
E dma@dma.org.uk
W www.dma.org.uk



Royal Mail Streamline

Streamline House
Sandy Lane West
Oxford, OX4 5ZZ
T (01865) 748768
F (01865) 780312
W www.royalmail.co.uk

**Advertising Standards Authority and
Committee of Advertising Practice**

Brook House
2 Torrington Place
LONDON, WC1E 7HW
T 020 7580 5555
F 020 7631 3051
W www.asa.org.uk

List Warranty Register (LWR)

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7321 3300
F 020 7321 4165
E dma@dma.org.uk
W www.dma.org.uk

List and Data Suppliers (LADS)

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7321 3300
F 020 7321 4165
E dma@dma.org.uk
W www.dma.org.uk

