



DMA Data Council
Data Best Practice Guidelines
2nd Edition

Acknowledgements

DQM, a data value management company, for their help in providing the data transfer guidance.

First Edition © The Direct Marketing Association (UK) Limited 2004.

Second Edition © The Direct Marketing Association (UK) Limited 2009.

Copyright © 2009 The Direct Marketing Association (UK) Limited. All rights reserved.

No part of this publication may be reproduced without the written permission of The Direct Marketing Association (UK) Limited.

Contents

	Introduction	3
	Why it's Important to get it Right	4
	Top Tips	7
	Why Best Practice?	12
1.0	Data Protection and Related Legislation	14
2.0	Caring for Personal Data	16
3.0	Data Capture	17
4.0	Receipt and Transfer of Data	21
5.0	Name and Address Cleaning	25
6.0	Name and Address Matching	30
7.0	Deduplication and Merge-Purge	34
8.0	Screening/Suppression	36
9.0	Data Tagging and Enhancement	43
10.0	Sortation and Output	45
	Appendices	
	Data Glossary	47
	Useful Addresses	49

Introduction

The contents of this guide are about providing advice and guidance on how to raise standards above the minimum of what is legislatively demanded of us, (what "has to be done"). This guide is designed to enable practitioners to achieve better results in an increasingly competitive marketplace.

The Direct Marketing industry faces one of its most challenging phases over the coming years. It must demonstrate to both Government and consumers that it has grasped the environmental gauntlet as well as convert an already tainted audience to the medium's benefits and advantages. This is not simply about changing our processes, such as using sustainable forestation as a paper source, or producing marketing materials that fully comply with recycling requirements. It is about doing business in a more consumer-centric manner.

Data is at the core of Direct Marketing; without it there would be no industry. However, it is also at the core of many of the problems facing us. Badly managed, maintained or captured data will lead to a catalogue of errors. It is important to remember that what might appear to you to be a trivial problem, to the recipient of the badly targeted mail piece, e-mail, text message, or phone call, it could be a ringing condemnation of our industry.

The issue of Data Security and ID Fraud will be around for many years. In many cases data is at the heart of these issues. That consumers feel confident and included within their relationships with brands is critical to both our longevity and success. How we respond to the challenges of Data Sharing (in light of the Walport Report) and how we provide consumers with increased confidence when it comes to the issues of protecting their identities against ID Fraud will determine the shape of our industry in the years to come.

All too often we forget to incorporate the views of consumers into our business practice, yet in fact without them we would have no business. This guide will help you to be compliant and as a result, hopefully, more successful. Our goal is to help raise the bar to a level desirable to all those involved in the Direct Marketing industry.

I am extremely grateful to all those members of the Best Practice Working Group who have all worked so hard to bring the second edition of these guidelines to fruition along with those other contributors, including those who helped produce the first edition in 2004 without whose hard and dedicated work this second edition would not have been possible.

Mark Roy
Chair – DMA Data Council Best Practice Working Group

Why it's Important to get it Right

1.0 Data Protection and Related Legislation

The simple fact is that the Direct Marketing industry has to comply with the law. Legislation impacts all that we do as business people, but in the direct marketing industry the Data Protection Act 1998 is the key piece of legislation we need to abide by. The legislation is designed to protect the rights of the individual and ensure that any data that is held on them is both accurate and up to date. The Information Commissioner's Office (ICO) takes a strong stance on ensuring compliance and the courts have fined a number of organisations for breaches of the Data Protection Act 1998. The high profile data losses and Government reviews in 2007 and 2008 mean data and data use will come under ever increasing legislative scrutiny.

Any organisation that fails to comply with the Data Protection Act 1998 leaves itself open to prosecution by the ICO and being fined by the courts. The ICO has recently been given new powers under the Data Protection Act 1998, although the relevant section is not yet in force at the time of writing (January 2009), to issue monetary penalty notices for breaches of the Data Protection Principles. There is also the risk of a private civil action for damages and reputation/brand damage.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 contain additional requirements for electronic marketing (phone, fax, email and SMS).

2.0 Caring for Personal Data

Consumer trust is one of the most valuable attributes an organisation can possess. In this time of identity theft and fraudulent activity it is critical that organisations take every precaution when handling personal data. Inadequate care and inappropriate handling of data has significant implications on consumer perception of a particular brand, with obvious implications for customer retention, as well as wider legal implications on the organisation.

3.0 Data Capture/ Consent

Through coverage in the media, consumers are becoming more and more aware of their data protection rights than ever before. With the volume of messages that they receive on a daily basis they are taking proactive measures when it comes to the management of these messages, including carefully choosing whether they opt-in or out of receiving them.

It is important to understand the implications of collecting data from various channels; telephone, email, mail, etc. To ensure that you are responding to customer wishes you must make it clear - for each channel - how the data will be used and what the expected outcome for the customer will be. This will ensure that you have satisfied customers; sending them information they are not only happy to receive but in some cases, information they have proactively requested.

4.0 Receipt and Transfer of Data

Any organisation receiving or transferring data must ensure that the individual's personal data is protected by appropriate security measures and processes, and that a data processing contract is in place.

5.0 Name and Address Cleaning

All Direct Marketing is about communication with an individual; therefore communicating with that person correctly and accurately is imperative. How you communicate with them is a reflection of how you feel about them. Maintaining accurate and up-to-date addresses on individuals is not only legislatively necessary but is simple common sense. Creating and maintaining accurate data files will allow you to ensure that matching for whatever purpose is most effective and will ensure that mailing pieces are correctly addressed, enhancing your reputation with the recipient.

6.0 Name and Address Matching

Receiving duplicate or incorrectly addressed communications is a major frustration for consumers. The experience can add to their negative perceptions of Direct Marketing, the organisation that sent it to them and the brand behind the campaign. Not least, they are increasingly concerned about the environment, which could add to their dissatisfaction and frustration over duplicate mailings.

Accurate matching of names and addresses in the campaign preparation process is a key element of effective DM to help reduce waste, increase response and build positive images with consumers for Direct Marketers and their medium. Equally, accurate name and address matching is important for ensuring that good prospects are not unintentionally 'suppressed' from the programme, which will also adversely affect results.

Best practice in name and address matching can be summed up as making sure you do all that you can to ensure the intended recipients receive only one copy of your mailing!

7.0 De-duplication and Merge-Purge

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

The actual process of de-duplication includes the identification of records that are considered to be the same and the selection of one of those records to be used or retained. The process is also referred to as merge-purge and dedupe.

The de-duplication hierarchy influences the end campaign's ROI (return on investment). Sending duplicate messages also damages brands and wastes money. Better planning equals better performance.

8.0 Screening

Screening your databases and mailing files for Gone Aways, deceased individuals don't want and opted-out individuals is crucial to a mailing campaign's success. The goal of most marketing activity is to target people who can respond. The British Direct Marketing industry wasted around £200 million in 2006 by sending mail to people who could not or would never respond.

In the current climate of consumer disquiet with the Direct Marketing medium, to mail Gone Aways and deceased people only serves to damage the entire industry's reputation and fans the flames of further potential legislation. Using suppression and data screening effectively will help protect the industry, improve your ROI and help present a more favourable environmental image to the outside world.

9.0 Data Tagging and Enhancement

By development of predictive models (which utilise all available data on consumers) clients can optimise the efficiency of their campaigns by selecting the best responding segments and therefore maximise response rates. Enhancing your customer file with additional data from external sources can often increase the effectiveness of these models.

For the consumer, this means that they are more likely to receive relevant offers or communications. Adding data such as date of birth or certain lifestyle characteristics can also be used to ensure a more personal message within the communication, thus providing the consumer with a more positive experience of the brand. This data can only be added if it is relevant to the product or service, otherwise there is the risk that the principle of only collecting and processing information which is relevant and not excessive could be breached.

However, it is important to ensure that external data is used appropriately and effectively and in accordance with the Data Protection Act 1998. The consumer must give permission for the organisation, which originally collected the information that you are using to enhance the customer file, to pass the information on to third parties. If the external data tagged to the customer's file is inaccurate or out of date, the consumer affected may feel annoyed or worse, and it may damage the customer's relationship with the brand.

10. Sortation and Output

Understanding sortation is essential to providing the best service possible to your customers. By using the most appropriate sortation sequence you will be able to provide significant cost savings depending on the offering from the postal carrier. Additionally, ensuring that the data is sorted in a manner that is going to provide the best results for the campaign is also very important. Ensuring that the customer receives the right message at the right time will build their confidence in the brand and help ensure an overall positive brand image.

1.0 Data Protection and Related Legislation

- Every organisation that processes personal data must notify the Information Commissioner's Office, unless they are exempt. Please see the Information Commissioner's Office Notification Handbook for details available from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/notification_handbook_final.pdf
- All DMA members must have an individual who is responsible for compliance with the DMA's Direct Marketing Code of Practice.
- The Data Protection Act 1998 gives individuals certain rights in respect of their personal data, including the right to make a Subject Access Request. A Subject Access Request requires the data controller to provide certain specified information and a copy of the personal data held within a maximum of 40 days from the date of the receipt of the written request and the payment of the fee (maximum of £10), if the fee is charged.
- Consumers also have the right to write to a organisation and ask it not send them any further Direct Marketing. This prevents you from processing their data again for Direct Marketing purposes. It is key that you continue to hold this data for suppression purposes to prevent further uses of this data, whether you are prospecting or marketing to known customers.
- In all cases, it is the most recent piece of information or instruction received from a consumer that takes priority.

2.0 Caring for Personal Data

- Customers are a business's most important asset, so taking care of their details is essential.
- Accuracy is crucial for best practice and to avoid wastage – use of address management software is a must.
- Personal data has to be secure – you must take appropriate technical and organisational measures to protect the security of the data. For example, you should consider password protecting and encrypting the data to limit access to relevant personnel only.

3.0 Data Capture

- Data planning for the ideal complete set of data required to be captured is key from the outset. However, you must remember that under the Data Protection Act you can only collect data that is relevant and not excessive to your processing requirements.
- Make the process of providing details as easy as possible:
 - In print, make sure spacing is correct (avoid free form where possible).
 - On the telephone, keep it as short as possible (use automation for speed).
 - With email/online, pre-populate data wherever possible (i.e. save details or use address finders).

- Remember that all sensitive personal data (see glossary) needs to be captured correctly on an opt-in basis and updated where necessary.

4.0 Receipt and Transfer of Data

- Ensure everyone in your organisation understands their responsibilities regarding the transfer and storage of data.
- Classify data so that individuals can recognise its importance and sensitivity.
- Send data via electronic methods, where possible, and ensure it is encrypted for security, whatever method is used for despatch. Passwords should be sent separately. Guidance on specific mechanisms to achieve this is supplied in the Receipt and Transfer section 4.0 on page 20 below.
- Ensure documentation is sent with all data, including file layouts and volumes.
- Make sure you receive "Proof of Delivery" of data.
- If you are receiving data files ensure you check them, in a timely manner, against the documentation to validate their contents.
- Store data in a secure environment, ensuring adequate backups and archiving takes place.
- Once processing is complete, return the data, following the secure methods described above, to the owner.

5.0 Name and Address Cleaning

- Send as much sample data as possible to the Data Processor to get a reliable estimate of the accuracy.
- Provide "raw" data - not pre-processed as this could diminish eventual accuracy.
- Provide an accurate layout as this will indicate to the bureau what is presented in each field and improve results.
- Provide as much information as possible – i.e. title, forename, middle name/initial, surname, suffix, full address, postcode, telephone number, date of birth, account number, URN etc.
- Define the data - e.g. consumer, business, customer, prospect, foreign, etc. This will help the bureau define the most appropriate processing.
- Provide data collection date to indicate the "age" of the data as this will give an indication of potential decay, which will help the bureau interpret results.
- Take advice from your bureau - they are experts in their field.

6.0 Name and Address Matching

- Be clear on the match purpose (de-duplicate, screen and enhance) and select the match routines that will best achieve these results.

- Develop a clear, written brief stating broader objectives, type and level of matching to be used.
- Select a bureau based on its relevant experience and need for flexibility of matching.
- Don't select a bureau on match volumes or price – consider asking for a fixed price for the job rather than price per '000' to reduce possibility of 'overmatching'.
- Understand your own and external data files that are being matched.
- Ask yourself, for your application: 'what is a duplicate?' Define it!
- Before matching, standardise, as far as possible, both the name and address records by using an addressing tool based on PAF and your rules for formatting key elements of the name. Similarly, introduce a clear process and rules (including rapid addressing software) for capturing data going forward.
- Undertake match tests and review results thoroughly. Use this experience to develop the most suitable routines. Check a sample of matching results to further verify results.
- For matched customer data (especially business suppression files) use the match as a 'trigger' to focus further research on a likely outcome of business record – don't just assume the business has closed.
- Review the finished results (at least a reasonable sample) thoroughly to help ensure data has been matched correctly.
- Lastly, in the event of getting a number of errors make sure you have a clear, easy and effective process to manage calls from recipients to get their details correct and entered on the database just once!

7.0 De-duplication and Merge-Purge

- Always visually check a random sample of data for quality and completion levels prior to processing.
- Don't just create de-duplication hierarchies based on price alone. Use net name rebates, previous response rates and data quality as well.
- Always standardise and format data prior to processing.
- View samples of duplicates and of the de-duplicated file prior to processing. Complete data audit trails may have to be provided to data owners and you need to be confident of the end results.

8.0 Screening

- Every file, whether current customers or historical enquirers, has some data decay on it. Data starts to decay as soon as it is collected.

- As a DMA member, you MUST use the Mailing Preference Service (MPS) Telephone Preference Service (TPS), the Corporate Telephone Preference Service (CTPS) and the Fax Preference Service (FPS) before contacting cold prospects. It may be of value to use it on existing customer files to screen existing customers who may not wish to receive mail or telephone communications, unless you are sure that you have consent to contact them for marketing purposes which will override registration on the appropriate preference service.
- For non-members the use of MPS screening is a requirement under the CAP code for cold prospect mailings, but in the opinion of the DMA and other industry bodies it is now also a legal requirement under The Consumer Protection from Unfair Trading regulations 2008 to screen against the MPS, It is however important to seek ones own legal advice on this specific issue. The use of TPS, CTPS and the FPS was always a legal requirement.
- You should determine which suppression files to use by assessing the value of the file that you are screening. The more valuable the data you are screening the more accurate you will require the suppression file to be.
- If you are screening a prospect mailing, and assuming that you have negotiated your net names arrangements correctly, you should screen the data against all suppression files which you, and your bureau if you are using one, have access to
- When determining a hierarchy of use for suppression files, cost or volume should not arbitrarily enter the equation. The best product would have 100% market coverage, be 100% accurate and would provide daily updates. How close it is to these three key criteria should determine where a product sits within a hierarchy.
- Whilst you must ensure you do not send Direct Marketing to those people who have asked not to receive it, at the same time be careful about over-suppression. More matches than is possible within the universal market are likely to be identifying people who have NOT moved or died.
- Postal returns sometimes do not indicate a Gone Away, but rather a disgruntled customer or prospect. In 1995 the average no-mail file had around 30% of supposed Gone Aways still living at the address. In 2005 this had arisen to around 42%. Consumers are getting wise to how the Direct Marketing industry works.

9.0 Data Tagging and Enhancement

- Be clear about why you are enhancing your file with external data (is it to improve targeting and selection to allow personalised messaging, etc?).
- If you are buying external data for use in targeting models, test which variables will give you uplift before buying.
- Retest data variables every year as the profile of your customers may change.
- Check how up-to-date the data you are buying is, e.g. when and how was it collected?
- If possible, check a sample of data where you already hold that information on your customers, to check how accurate that data source is likely to be.
- Make sure when matching the data you decide whether your matching level needs to be individual, household or location, and ensure that you minimise the possibility of confusing two individuals in the same household.

- Don't use modelled data for personalised messages; it will probably not be accurate enough.
- For modelled data, ask the supplier to give you confidence levels for the accuracy of the models.
- Use a control cell to determine the additional value the enhanced data is supplying

10. Sortation and Output

- Investigate data sequence sortation options before choosing a method.
- Data should be processed based on requirements of scheme.
- Segment final mailing based on the client's selection criteria.
- Provide early consideration to the final output required and discuss with the bureau, the mailing house or printer and the email or fax broadcaster.
- Provide supply of test data to printer to allow sign off of a sample print.
- Refer to Royal Mails mail processing guide; Know How (the user's manual for Mailsort®, Presstream®, Walksort®, Presstream® Walksort®, Cleanmail®, Royal Mail International Bulk Mail™ and Automated Standard Tariff Large Letter)

Why Best Practice?

The use of data is key to most, if not all, 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 11% of the population moves address each year: Office for National Statistics 2006.
- Approximately 11% of addresses are mailed incorrectly each year: Direct Mail Information Service (DMIS).
- 45% of the UK population believe that a misspelt name or address is an indication of 'junk mail': Direct Mail Information Service (DMIS).
- 4,232,649 UK households (as of December 2008) 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 are maintained to the highest standards (please refer to Section 4.0: 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 misspelt 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 that are included in the DMA's Direct Marketing Code of Practice and specific legislation. The Data Protection Act 1998 is the principal legal framework that governs how all personal data must be processed. The Privacy and Electronic Communications (EC Directive) Regulations 2003 contain additional rules for electronic marketing (telephone, fax, email and SMS). These guidelines set out where responsibility lies between clients and bureaux for ensuring compliance with the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003 at each stage of data usage.

The outcome of following these guidelines should be better-performing communications that build customer relationships and long-term loyalty. These are objectives that the whole industry share, and which the Data Council and the DMA endorse.

1.0 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.

Public domain information can only be used for the purpose for which it is provided. Every item of data used must have been given freely and voluntarily by the customer, 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. To maintain best practice in the use of data, marketers must have in place facilities to ensure that data is accurate and up-to-date, 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.

Unsubscribe requests not to be mailed, phoned, faxed, emailed or texted by a particular organisation (separate from Mailing, Telephone, Corporate Telephone and Fax Preference Service registration) sent directly to the data user or the list owner should be logged on in-house 'Do not mail', 'Do not telephone', 'Do not fax', 'Do not email' or 'Do not text' suppression files and contact lists should be screened against the relevant in-house suppression file as well as the appropriate Preference Service file before sending out any marketing communication. For more information on:

- Email, please refer to the Email Marketing Best Practice Guidelines, [click here](#).
- SMS, please refer to the Mobile Marketing Guidelines, [click here](#).
- Privacy and Electronic Communications (EC Directive) Regulations 2003, [click here](#).

1.1 Responsibilities

The client is responsible for ensuring that:

- It has registered as a data controller with the Information Commissioner's Office.
- Where processing of personal data is carried out by a bureau on behalf of a client, the client must 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.
 - b) Take reasonable steps to ensure compliance with those measures.
 - c) Have the processing carried out under contract:
 - i) Which is made or evidenced in writing.
 - ii) Under which the bureau is to act only on instructions from the data controller (Please [click here](#) for a link to the suggested DMA data processing contract and guidelines).

d) The contract requires the bureau to comply with obligations equivalent to those imposed on the client by the seventh principle of the Data Protection Act (see paragraph above).

- 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, Sales Promotion and Direct Marketing (the CAP code).
- Facilities are in place for updating data, registering unsubscribe requests not to be mailed phoned/faxed/emailed/texted and to permit access to their own personal data by each individual.
- Third-party data rented from any data supplier is supported by a list owner warranty.

The supplier is responsible for ensuring that:

- The data controller has fully and correctly registered with the Information Commissioner's Office (all current notification details are now accessible online at <http://www.ico.gov.uk/ESDWebPages/search.asp>)
- 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), Corporate Telephone Preference Service (CTPS) or Fax Preference Service (FPS) and consideration of other screening files is made.
- Any communication using data they own/manage complies with the British Code of Advertising, Sales Promotion and Direct Marketing (the CAP code).
- Unsubscribe requests to be removed from a marketing list, to have details corrected, or to have access to the information held are properly dealt with.
- List owners hold a list owner warranty.

Prompt action must be taken to respond to a customer request in writing for access to his or her personal data. Under the Data Protection Act 1998 a copy of all personal information held has to be provided promptly and in any event within a maximum of 40 days from the date of receipt of the written request and the payment of the fee, if required. The current maximum fee is £10. Such requests should be dealt with as a customer service query in a spirit of transparency and good faith, bearing in mind the legal requirements.

2.0 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 of the amount to sell to an existing customer as it does to make a sale to a new customer. During the course of a customer's lifetime with a company, 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 comply with legislation and also maintain the 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:

- The **data capture process** should be given particular attention. Please see the first principle of the [Data Protection Act 1998](#) (see also [Schedule 1 Part 2](#) and [Schedule 2](#)). In summary individuals must be told the purposes for which their information will be processed and given the appropriate opt-out or opt-in options.
- **Sensitive personal data** under the Data Protection Act 1998 has special rules that apply (see [Schedule 3](#) of the 1998 Act).
- The **management of personal data** should be underpinned by the [fourth principle](#) of the Data Protection Act 1998. 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 bureau.
- Data security is detailed in the [seventh principle](#) of the Data Protection Act 1998. You must take appropriate technical and organisational measures to protect the security of the data. For example, your business procedures should ensure that: no customer or prospect listings are left lying around or discarded in waste bins which could ultimately end up in the wrong hands or in the public domain, computer screens displaying personal data are not visible to unauthorised personnel, and when handling enquiries by phone, which may result in personal data being discussed or revealed, the identity of the person at the end of the phone is verified.

Section 8.0 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](#).

3.0 Data Capture

To make use of data – whether name, address, telephone number, email address 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 online (websites or email).

3.1 Printed response

When designing a marketing communication that 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, mail shot, 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 assignment 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.
- Test a coupon before signing off on a campaign by asking a friend or colleague to complete it.

3.2 Telephone response

Telephone response gives an ideal opportunity for data capture of name and address as well as other information, subject to time and cost constraints and relevant legislative requirements and best practice 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 automated 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.

Be careful when asking open ended questions as these can extend call times and can be difficult to analyse. Yes/No questions, banded information or multi-choice responses are quicker to capture and easier to analyse.

- Telephone response mechanisms must:
- Ensure that the respondents are told the purposes for which their personal information will be used either via the IVR or live operator call scripts.
- Offer respondents a mechanism to opt-out of receiving further unsolicited direct marketing either via the IVR or live operator call scripts. Such opt-out requests should be processed in accordance with section 1.0 Data Protection and Related Legislation (see above p13). If possible such opt-out mechanisms should allow respondents to opt out of receiving unsolicited direct marketing via particular channels.

For more information about the legal obligations relating to electronic communications please see the [Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#)

3.3 Fax marketing

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

- Ensure that no unsolicited marketing fax is sent to a consumer or business operating from a consumer premises, unless the marketer has the prior consent of the recipient.
- 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 marketer or fax broadcaster acting on the marketer's behalf.
- Ensure that the fax number of such 'do not fax' recipients are removed from the respective fax lists and added to the in-house 'do not fax list' in a timely manner after notification and not called in future campaigns.
- Ensure that any consumers, or businesses operating from consumer premises, are made aware of the Fax Preference Services (FPS) contact details (see Useful Addresses) 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 broadcast is diligently used in a timely manner to maintain up-to-date fax lists for future use.

3.4 Electronic media

The growth in 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 nature of these media.

Electronic media also provide an excellent opportunity for customers to maintain their own data either through e-mailing requests to update their records, being asked when calling in or being prompted to go online to change details.

It is recommended that members consult the [DMA Email Marketing Best Practice Guidelines](#) and/or [DMA Mobile Marketing Best Practice Guidelines](#) for more detailed information.

3.5 Using data capture bureaux

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 that is identical to the responses received, with information exactly as provided by respondents. In the second stage, the 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 needed 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 Data Protection Act 1998](#), which governs the transfer of data outside the European Economic Area. To comply with the law, data will only be allowed to be exported outside of the European Economic Area to countries that have an adequate level of data protection or where contractual arrangements are put in place between the organisations involved that ensures an adequate level of data protection. Members must 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 individuals, or where an alternative means of ensuring adequacy exists, such as through an appropriate contract. A Safe Harbour Agreement currently operates between the US and Europe. US firms operating under the Safe Harbour Agreement pledge to protect data from European partners in accordance with European law. For up-to-date information about which countries have been granted adequacy status please visit http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm Members transferring data out of the European Economic Area are strongly advised to consult the [DMA's Legal Department](#) or their own legal adviser's.
- 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.

3.6 Benchmark

The level of accuracy for data capture should be agreed in advance between client and the bureau. 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 are 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.

3.7 Responsibilities

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, stored securely, and once the work is complete, are returned or disposed of in line with the Data Protection Act 1998, and the client's brief.

4.0 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.

As best practice, an individual's data should be treated as confidential. You must ensure at all times that an individual's privacy is protected and the obligations imposed by the Data Protection Act 1998 are followed **as a minimum**. If in doubt as to the classification of any data, err on the side of caution and use the default of 'Confidential'.

All transfers, handling and storage of data must 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 must ensure data will be held securely and files processed lawfully, so that only the appropriate people can access the data. Data should always be backed up and archived.

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, 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 must 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/DVD 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. Re-supply of data will be necessary if a file does not tally with the documentation, or if it is corrupted.

The seventh principle of the Data Protection Act 1998 states:

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This applies to you even if your business uses a third party to process personal information on your behalf.

4.1 Data Transfer Guidance

The following guidelines have been prepared by the DMA List and Insert Forum with guidance and support from a member company. They are intended to offer a minimum requirement for the technological processes that should be followed by DMA members for transferring data between 2 locations. The aim is to ensure that all parties in the chain of data transfer are following these basic minimum recommendations.

The guidance does not address legal, compliance or any other procedural legislation but is simply an attempt to provide some basic best practice advice on technological measures to protect the security of data transfer. It only covers recommendations for data transfer between countries within the European Economic Area (the 27 Member States of the EU,

plus Iceland Lichtenstein. For data transfers to other countries please see section 3.5 on page 20 above..

Before Transfer

Before the transfer of data is undertaken it is advisable to consider:

- a) Is the transfer really necessary? Don't move it unless you really need to!
- b) Are you transferring more than is needed? Reducing the amount of data moved reduces the risk and consequential damage if lost – This could mean sending only those records that are needed or only those fields that are required.
- c) Are you confident that the recipient of the data is authorised to receive and process the data?
- d) Do all parties have the correct Data Protection notification?

Having ascertained that a transfer is required and reduced the data to the minimum necessary it is important to consider HOW the data is transferred. Many methods of moving data from place to place are available but the main ones to consider are as follows (they have been listed in order of preference for guaranteeing the maximum level of security) –

Secure FTP (or SFTP)

This method is a point-to-point transfer from client to server. Data is transferred directly from one machine to another and is encrypted throughout the journey. All the data is encrypted before it is sent across the network. With SFTP sending usernames and passwords in clear text is a thing of the past, and all transferred data is fully encrypted. Furthermore this is completely transparent to the user and the way the application behaves is the same.

SFTP Software is available at reasonable cost from many suppliers.

It is recommended that the files to be transferred are compressed and separately encrypted before transfer (see above comments) – this is so that access to the data is still controlled once on the destination server. Several software applications are available for this. Passwords used for both the SFTP session and the File Compression should be unique and strong – by that we mean at least 8 characters, containing both numbers and letters and not based on a dictionary word. Ensure that passwords are exchanged separately and securely. Passwords should also expire after a suitable time period and data should be removed from servers as appropriate.

With passwords it is recommended that when required, data file(s) are compressed and password protected before being transferred. The password should contain at least 10 digits of which 2 digits should be lower case, 2 should be upper case, 2 should be special characters, 2 digits should be numbers and the 2 digits can be any of the aforementioned digits.

FTP

FTP is a point-to-point transfer from client to server. Data is transferred directly from one machine to another but the transfer is NOT encrypted. All data is passed back and forth between the client and server without the use of encryption. This does make it possible for an eavesdropper to listen in and retrieve confidential information including login details

This is not as secure as SFTP but if the remaining guidelines below are followed is probably better than the alternative methods listed.

It should be mandatory that files to be transferred via FTP are compressed and separately encrypted before transfer – this is to protect the data if intercepted in transit in addition to the reasons listed above. It is even more important that the rules above relating to passwords and removal of data are followed.

Physical Transfer by Courier or Post

Cutting CDs/DVDs and tapes and other media forms can mean that data gets misplaced or delivered to the wrong person. If this is the only method of data transfer available then the following guidelines should be followed:

- Ensure that the data is minimised (depersonalised if possible!).
- Protect the data with strong encryption (AES256 is good).
- Strong and unique passwords sent separately to the recipient.
- Use a courier with a specific data service if possible.
- Have a good contract with the courier service – if this is to be regular and the data is high value consider asking to see the courier's security policies.
- Confirm delivery with the client.
- Ensure that signatures and receipts are readable and available quickly.

E-Mail (as an attachment to normal mail)

This is not desirable and should be avoided if possible. The main problem with e-mail is that in most cases the message is not transmitted directly from sender to receiver – there may be several server-to-server hops for the message – each one of which is a potential resting place for a copy of the original message. Additionally a copy of the data sent is likely to remain in the accounts of the sender and recipient and on the mail servers of the respective locations. If this kind of transfer is unavoidable then the following guidelines should be undertaken:

- Ensure that the data is minimised (depersonalised if possible).
- Protect the data with strong encryption (AES256 is recommended) before attachment.
- Strong and Unique passwords sent separately to the recipient (preferably by telephone rather than another email message).
- Ask for a tracking receipt so you know when the email is opened.
- Delete the attachments/sent email after the message receipt is confirmed.

4.2 Responsibilities

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 and a data processing agreement is in place. [Click here](#) to download a draft data processing contract.
- 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.
- 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.

5.0 Name and Address Cleaning

In order to carry out effective record matching for the purposes of de-duplication, 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'.

5.1 Data Formatting

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.

There is no common standard for the way organisations format their name and address data. As such, a process is required to help tidy up formatting - such as separating name and address lines, removing non-address text or any other erroneous data that cannot be used for matching or de-duplication purposes.

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 are as good as possible, as detailed below.

5.2 Name Cleaning

It should first be established that 'name' data is present and correct in the record. Where an address is supplied but name data is not present, or where the processing has been unable to separate a surname from the other name fields, input records should be rejected or flagged for default salutation.

Bureaux 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.

5.3 Name parsing

As no assumption can be made that the various elements of a 'name' field will be presented separately, bureaux should be able to identify separate name elements and parse them into their correct fields, i.e. prefix, title, forename/initial, middle name/initial, surname and suffix. Care must be taken to ensure that double-barrelled surnames are treated as a single field.

5.4 Title/Salutation and Suffixes

Bureaux should 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.

5.9 Address Cleaning

Bureaux should establish that address data is present in the record. Where no address data is available the record should be rejected for mailing purposes and or flagged.

5.10 PAF

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 unique address or delivery points and postcodes within the UK, including England, Scotland, Wales, Northern Ireland, Jersey, Guernsey and the Isle of Man - approximately 27.5 million records. Following formatting the next stage is usually to match all records against the PAF file, which contains the generally accepted correct address presentation.

This is usually a dynamic process, which typically involves:

- Identifying records, which exactly match PAF.
- Retaining client-preferred address elements, e.g. unregistered house names.
- Correcting poorly formatted addresses to bring them up to PAF standard or to a point where the record is capable of being delivered.

Bureaux should have the ability to correct inaccuracies in addresses to improve the chances of them matching to PAF. Bureaux will have different capabilities depending on their software. However, the following are likely to be included:

- 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.
- Matching old postal geography to new.

e.g. 1:

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.

e.g. 2:

BIMRINGHAM	- becomes -	BIRMINGHAM
CRODON	- becomes -	CROYDON
MANNCHESTER	- becomes -	MANCHESTER
GUISELEY LS20 8HU	- becomes -	GUISELEY LEEDS LS20 8HU

- Recognising common edit marks.

e.g. 3:

STOKE ON TRENT	- and -	STOKE-ON-TRENT
SOUTHEND/SEA	- and -	SOUTHEND-ON-SEA

- Correcting common abbreviations and superfluous words.

e.g. 4:

BRUM - becomes - BIRMINGHAM

HANTS - becomes - HAMPSHIRE

Dulka Road, 'betwixt the commons' - becomes - Dulka Road

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.

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 bureaux and clients in a number of different formats and bureaux should adopt these changes within a 'reasonable' amount of time. A good benchmark is that they are adopted within three months of the changes being made.

5.11 Level of Address Verification to PAF

Whilst all bureaux should have a standard minimum criterion that records must fulfil to match PAF, it is desirable to offer a bespoke service whereby clients are able, following consultation, to tailor this criteria to their specific requirements.

5.12 House Names/Numbers

Bureaux should be able to discern the various presentations of house numbers and or names. This should include the identification and correct manipulation of complexities, such as flats and sub-premises.

5.13 Business Data

The principal 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:

5.14 Contact name/Company Name

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

5.15 Job Title

Records may also contain job title information e.g. Fred Smith, Tester, Manufacturing Department, Bloggs and Co, 1 The High Street, Maidstone ME15 1SA.

5.16 Departments

In the above example the department name would be, 'Manufacturing Department', almost certainly an additional element to the PAF supplied address.

In addition, the party providing the input data should consider how to set business rules to govern whether the company name as it appears on PAF should replace the input name.

5.17 Overseas Data

To ensure successful foreign name and address data processing the chosen bureau should have a certain familiarity with local idiosyncrasies specific to each set of country data being processed. This would require 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.

5.18 Reporting

Bureaux should provide comprehensive reporting of any and all alterations to input name and address records at each stage of the process, with explanations for changes being supplied.

5.19 Responsibilities

To ensure that any data cleaning project is carried out to the client's satisfaction and to the best of the ability of the bureau; both parties must consider their individual responsibilities:

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 are business or consumer data and whether they contain 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.

6.0 Name and Address Matching

The matching of 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 Telephone Preference Service (TPS), or Fax Preference Service (FPS) is required by legislation for unsolicited direct marketing calls and where a communication is unsolicited Direct Marketing matching against the Mailing Preference Service (MPS) is required under the DMA's Direct Marketing Code of Practice and the CAP code. It is the opinion of the DMA and other industry bodies that it is now a legal requirement to screen against the MPS under The Consumer Protection from Unfair Trading Regulations 2008, It is however important to seek one's own legal advice on this specific issue. In the business-to-business sector, matching against the Corporate Telephone Preference Service (CTPS) is now a legal requirement for all unsolicited telemarketing campaigns.

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 standardise addresses and identify ambiguous addresses and offer alternatives. Typical difficulties arise out of misspelt addresses that could be resolved into either of two places. Boston, Lincs and Bolton, Lancs are commonly confused.

INCOMING ADDRESS:

MATCH ONE:

2 Church Road
Bolton
Lincs
BL4 8AL

MATCH TWO:

2 Church Road
Farnworth BOSTON
BOLTON Lincolnshire
PE21 0LW

Different matching rules should be considered for the 3 different applications.

Where data is to be suppressed or enhanced, there are risks associated with matching. Removing a record that appears to be a duplicate, but which in fact is just very similar, such as an identical surname in the same household, 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.

6.1 Matching Levels

Where no data is to be overlaid, matching and de-duplicating a file is usually carried out with a level of overkill – suppressing even doubtful duplicates in order to reduce wastage. Under kill 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 record 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.

6.2 Consumer record matching

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

- Matched on title, initials/forename, surname and address.
- Matched on surname only and address.
- 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.

6.3 Business record matching

Matching business data is far more complex due to the much broader variations in names, abbreviations, multiple occupancies and trading versus registered addresses. The fact that a business customer will generally have a higher value than a consumer adds to the importance of getting the results accurate.

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

- Matched on contact name and company and address (Contact at Company Site Level).
- Matched on company and address (Company Site Level).
- Matched on address only (Site Level).
- Company name only.
- Phone number.

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. Equally, several businesses with very similar names may trade at the same address but be different legal and trading entities. Also, one or more might be registered offices, holding or dormant businesses.

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, or run routines that are able to identify these as matches, for example, recognising International Business Machines and IBM as the same company.

Special attention needs to be taken with company name matching to take into account the context of the match – for example, if matching is being undertaken to identify the same legal

entity then very close name matching must be used - i.e. IBM Ltd may not be the same legal entity as IBM (UK) Ltd.

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

The more recent introduction of business suppression files has highlighted the problems associated with matching business addresses, as incorrectly suppressing a live customer can be very expensive. When using a bureau or specialist software, clients should verify their B2B experience/capability prior to instruction.

Clients should look closely at match levels, accuracy, name formats/spellings and matching trading names against registered details. Whilst as important as best practice in consumer suppression, we recommend that users should use business suppression with great care, primarily as a means of identifying likely out of business records, and as a trigger for focusing research to update the record.

When matching prospect data, clients can take a less conservative approach but must still remember their obligations under the Data Protection Act 1998.

6.4 Non-name and address matching

Another option available in a de-duplication 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 that has a high level of population on the files being matched.

6.5 Responsibilities

The client is responsible for ensuring that:

- A clear 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. Request a test exercise and a review session of results to work with the bureau to obtain the most suitable results depending on the application.
- Further information requested by the supplier is supplied in a timely fashion.
- A data audit (i.e. a sample of file with verification of matching), if requested, is signed off promptly. The client should look closely at the match results and surrounding issues to ensure a satisfactory level of accuracy.

The supplier is responsible for ensuring that:

- A clear brief has been received and understood and any special processing requirements have been clarified and agreed.
- Match rules and hierarchies are used according to the brief with sample matches supplied if required.
- Any problems with the data received are advised to the client as soon as possible.
- 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.

Last, but not least, we recommend that clients look closely at their data capture processes and systems. Again, by standardising name and address formats in tune with recommended best practice, matching results will be improved over the long term.

7.0 De-duplication and Merge-Purge

7.1 Hierarchies

To carry out the de-duplication 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, de-duplication 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 de-duplication 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 Response First: This produces the most cost effective list. This is only possible 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. De-duplication 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.

7.2 Duplicate identification

The de-duplication 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:

- One per person.
- One per address.
- One per household (or surname at address).

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

- One per job function (better than job title if it is available).
- One per site.
- One per company.

It is essential to understand the actual composition of your data file when setting your de-duplication options. For example, choosing to select one per job function when only 25% of the records on the file contain job functions is a non-starter!

Many clients recognise they require different standards of de-duplication depending on the information 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.

Then there are issues with errors, or non-standard formats, which will inhibit duplication identification, e.g. Antony, Anthony, Tony, T or A. To minimise these variations, it is best to

standardise and format the data prior to de-duplication. This will then influence the level of match accuracy that can be, or needs to be, achieved.

A hierarchy of matching accuracy, from least to most precise is as follows:

- Address.
- Surname + address.
- Initial, surname + address.
- Gender, initial, surname + address.
- Gender, forename (soundex), surname + address.
- Gender, forename (soundex), surname (soundex), + address.

Soundex allows typing errors to be ignored in the identification of matches, providing the sound of the name doesn't fundamentally change.

Match accuracy levels should be determined by the business requirements, and the data quality (see section 6.0 for more detail).

Net name rebates are affected by where in a hierarchy the list is introduced for de-duplication. The later in the process, the higher the number of duplicates 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 de-duplicated file, must also be supplied.

7.3 Responsibilities

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 de-duplication 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 that 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.

8.0 Screening/Suppression

Suppression files are playing an increasingly important role in the effective management of marketing communications for a wide variety of organisations.

At a very simple level, these files **contain the records of people that cannot or do not wish to respond to personalised mailings or other targeted marketing communications.**

They can also include people or businesses that are unlikely to respond or are unlikely to be creditworthy or are deceased or have moved.

Suppression information is used by organisations to literally 'suppress' some of the records selected for marketing purposes or alternatively to enhance or recover the information held on an individual or business.

There are several types of information contained in consumer suppression files:

- People who have moved address - known as "Gone Aways".
- People who have died.
- People who have requested 'no contact' (by mail, phone, fax, email or text messaging).
- People who may represent a credit risk.

Equally, there are similar types of information contained in business suppression files:

- Businesses that have moved address.
- People whose employer has changed.
- People whose functions have changed within a business.
- People who have died.
- Businesses that have changed name.
- Businesses that have ceased to trade.
- Businesses that have requested 'no contact'.

Apart from the obvious exceptions, most people or businesses either forget or choose not to notify the above changes to organisations that hold their details on file.

8.1 So how and why does suppression affect me?

What is clear from the following summary statistics - compiled from industry and government sources - is that data decay cannot be avoided, therefore the use of suppression is critical to your success and remaining compliant to both the Data Protection Act 1998, the DMA's Direct Marketing Code of Practice and the CAP Code.

Consumers

There are approximately 60.6 million people living in the UK (46 million being adults aged 18+) (2006).

Around 575,500 of these adults died in 2006 – 0.9% of the population.

They reside in approximately 24.2 million households (2006).

11% of the population moves each year, approximately 6.6 million people (2005).

4,002 million items of direct mail were mailed in 2005.

On average each British household receives 13.2 items of Direct Mail every 4 weeks and spends approximately £590 through Direct Mail per annum

Only 7% of this mail is requested.

Two thirds of the British public either throw direct mail in the bin or want to stop it completely.

(Sources: Office for National Statistics, DMIS and MORI Research)

Businesses

There are approximately 1.67 million VAT registered businesses, (estimated 4 million total businesses in the UK) (2007).

1,132 business mailings were sent in 2005, accounting for 23% of all Direct Mail.

Approximately 30% of these business records are incorrect within one year.

On average, Business Managers receive 728 mailings every year.

On average, each Business Manager receives 60 items of direct mail every month.

(Sources: DMIS Letterbox Factfile 2006, ONS 2007)

Without exception, it makes sound commercial sense for organisations using any form of direct marketing to keep up-to-date with the changes taking place every day in the UK population and amongst UK businesses. It is now well documented and broadly accepted that organisations ignoring the issue of data decay will not be able to compete effectively against those that do keep their data up-to-date and accurate.

From a marketing perspective, suppression files are used for a variety of purposes:

- To help eliminate a wide range of direct and indirect costs associated with sending mail to people that cannot or will not respond.
- To enhance the data held on customer files by attaching flags.

- To help businesses identify Gone Aways as a first step towards re-establishing contact with their customers.
- To improve the efficiency of mailing and telemarketing.
- To help identify significant changes at either individual or address level, which can be used for targeting purposes.
- To assist with credit checking.
- To help charities identify legacy income.
- To comply with legal requirements and 'best practice' guidelines regarding the privacy rights of individuals and businesses.

"Personal data shall be accurate and, where necessary, kept up to date".

(Source: Data Protection Act 1998)

For further information see www.informationcommissioner.gov.uk

It is a legal requirement for all marketers to use the Telephone Preference Service, the Corporate Telephone Preference Service, the Fax Preference Service and their own in-house do not contact lists in the case of unsolicited Direct Marketing. Marketers should also remember that it is a requirement of the CAP code to screen against the Mailing Preference Service in the case of unsolicited Direct Marketing. In the opinion of the DMA and other industry bodies it is now a legal requirement to screen against the MPS under The Consumer Protection from Unfair Trading Regulations 2008. It is however important to seek one's own legal advice on this specific issue. You should remember that you do not need to screen your list of existing customers against the preference services, provided you have offered them an opt-out from direct marketing and you screen against your own in-house do not contact list before any unsolicited direct marketing activity. Members of the DMA should also note that use of the Preference Services is a requirement of the DMA Code of Practice.

8.2 DMA Suppression Files

Within the context of self-regulation, the DMA administers the Mailing Preference Service that allows consumers to stop unsolicited sales and marketing communications by Direct Mail – see www.dma.org.uk.

Registration with each Preference Service is free.

8.3 Mailing Preference Service (MPS)

The MPS Consumer File is a list of names and addresses of consumers who have expressed a wish to limit the amount of Direct Mail they receive.

The MPS is primarily used for suppressing consumers from 'cold' unsolicited mailing lists. There is no legal requirement to use MPS against existing in-house customer files, provided consumers were offered the opportunity to opt-out from further unsolicited Direct Mail marketing communications at the time of data collection and that the list of consumers to be mailed is screened against your own in-house do not mail list before each mailing. However, its use is a condition of the DMA's and the CAP Codes of Practice, and, in the opinion of the DMA and other industry bodies, is now a legal requirement under The Consumer Protection from Unfair Trading Regulations 2008. It is however important to seek one's own legal advice on this specific issue.

Over the last decade, thousands of consumers have registered with the MPS; this has increased even further with the availability of online registration and changes to the Electoral Roll. Names

remain on the file indefinitely or until the MPS is notified by the subscriber to remove them. The file is updated on a monthly basis; the current (December 2008) file size is in excess of 4 million with approximately 30,000 new records added each month.

The MPS Consumer File is held by most bureaux that usually provide suppression matches to their clients without charge.

It is important to note that historic MPS names are suppressed at a **household** level (same surname at an address). Since September 2007 new registrations have been at individual level.

MPS is funded through a levy on Royal Mail's Mailsort service and a licence fee collected through the licensees who purchase the data file.

8.4 Telephone Preference Service (TPS) and Corporate Telephone Preference Service (CTPS)

This is a list of individuals who have registered their telephone numbers to stop receiving unsolicited telephone marketing calls. Registration remains in place until an individual changes their telephone number. Current (January 2009) file size is approximately 14 million and is still growing at a significant rate. TPS files are only available to bureaux or end users through payment of licence/subscription fees.

When the TPS was first introduced in 1995 it was available to end users on a voluntary basis. In March 1999, Government legislation came into force which made it unlawful to make a call to an individual who has indicated that they do not wish to receive such calls; this can be either by notifying an organisation directly or as a result of registration with the TPS. Registration, however, will not stop calls from market research organisations, customer service calls and debt collection calls that fall outside the scope of the legislation.

Telemarketing companies must comply with a request for the suppression of a telephone number no later than 28 days after a registration with the TPS has been made. As a consequence the TPS file is updated daily.

All those in business (including charities, voluntary organisations and political parties) who make unsolicited direct marketing telephone calls to individuals must comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003. Both 'cold' lists and customer lists should be cleaned against the Telephone Preference Service before calls are made to ensure compliance with the Regulations, unless the existing customer exemption applies (see below.)

If a breach of the regulations occurs it is the responsibility of the Information Commissioner's Office to enforce the regulations. The TPS itself will investigate initial complaints made to it about a unsolicited marketing call made to a number registered on the TPS, but the Information Commissioner's Office will determine what action it will take for breach of the Regulations.

Whilst the scope of the legislation covers calls made to both 'cold' and existing customer lists, there are existing customer exemptions. You do not have to screen your existing in-house customer list against the TPS, provided that all the following conditions are met:

1. You have collected the telephone number directly from the consumer and not from the BT Osis or another file.
2. You told the customer that the telephone number will be used for unsolicited Direct Marketing activity.
3. You have provided the customer with an opportunity to opt-out from receiving such calls.

However, many organisations choose not to telemarket to individuals on TPS even if they have met the existing customer exemptions and are legally able to. It would seem fair to assume that an individual sufficiently motivated to register on TPS is not likely to respond positively to a

telemarketing call from any party. It would be best practice to use another communication channel to contact the customer.

The current legislation governing the TPS is the Privacy and Electronic Communications (EC Directive) Regulations 2003.

In 2004, the Corporate Telephone Preference Service (CTPS) was established. This is run in the same way as the TPS, except there are minor differences with the registration process. The CTPS allows corporates (limited companies and public limited companies in England Wales, Northern Ireland and Scotland and partnerships in Scotland as well as government departments and other similar organisations) to register their telephone numbers. The registration has to be in writing and renewed every year. The CTPS will also send out a confirmatory notice in writing of registration.

8.5 Facsimile Preference Service (FPS)

This is a register of individuals and businesses that object to receiving unsolicited direct marketing faxes.

Under legislation first introduced in May 1999, it is unlawful to send a fax to an individual unless you have their prior consent. The term 'individual' in UK law includes consumers, sole traders and partnerships (except in Scotland).

Organisations also have the opportunity to register fax numbers on the FPS that they do not want direct marketing faxes sent to.

Organisations using fax marketing must not send unsolicited fax marketing to fax numbers registered on the FPS no later than 28 days after the request was made. As a consequence the file is updated daily.

The scope of the legislation covers calls made not only to 'cold' lists but also to customer lists.

The current legislation governing the FPS is the Privacy and Electronic Communications (EC Directive) Regulations 2003.

8.6 Industry Suppression Files

Over the last few years, rafts of new products have entered the very busy suppression marketplace. Whilst this is positive in some respects, it has added to the confusion over the product that best serves the consumer.

Specialist companies use a range of different methods and sources for compiling suppression files, which are then made available to end-users, mainly through data processing bureaux that license the data. Some high volume mailers choose to have direct licensing arrangements with the file owner.

Most bureaux have a suite of different suppression products available to end-users. Some of these files offer similar data but use different sources and methods to compile the data.

As part of any standard data hygiene or mailing preparation process, end-users can be advised by their bureau of any records on their mailing or customer files that 'match' records on these suppression files.

Once a suppression match has been identified, the end-user can make an informed choice about the way in which the record is processed by the bureau, for example, whether records are suppressed or not.

The processes used by bureaux to identify exact or suspected matches is a topic which promotes much discussion as there are substantial differences in data processing techniques and matching

routines. These differences used to 'match' identical or similar records on mailing and suppression files account for most of the variations in results amongst bureaux matching on identical data sets.

The key criteria to look for in a product are market coverage, accuracy and speed. The perfect Gone Away product would identify all home movers - 100% accurately - immediately. Whilst in reality this is never going to happen, how you assess a product should be based on how close the product is to this ideal.

8.7 Market Coverage

This provides a measure of the value that a product can provide. 6.6 million people move each year, therefore a product collating 1.65 million individual records a year will only ever be able to provide part of the Gone Away suppression solution.

8.8 Data Accuracy

Data for suppression files is obtained from many sources. Some of these sources are verified, so a change in circumstance is known to have happened, e.g. a death registration number, others are assumed, e.g. multiple postal returns.

Inaccuracy in suppression files will "over" suppress, and remove records from your database or prospect file that HAVE NOT gone away. For example, whilst some postal returns clearly have been legitimately returned by new occupiers, a proportion (research shows around 40%) are sent back by consumers as a way of trying to get their names taken off a database.

It is therefore important to test suppression files for accuracy as well as match rates. The value of the data being screened should also be taken into consideration. Customer and prospect data may be treated differently due to the value of the historic relationship.

8.9 Timing

Timing is everything. The longer it takes for you to know that someone has died or moved, the more damage you will do to your brand and the smaller the savings will be. Of course, if you only mail once a year this issue is less important. However, if, like many companies, you mail on a monthly basis you need a suppression solution that fits your marketing activity. Most Gone Away solutions are now monthly, and deceased solutions are getting faster with one supplier now providing daily updates.

The use of suppression is an important and essential part of the legal and self-regulatory requirements. The Data Protection Act 1998 obliges you to keep your data accurate and up to date. This is clearly an undefined requirement, but doing the bare minimum will only serve to minimise the benefits available. There is a major environmental contribution to be made, in that sending mail to people who are never going to respond wastes an enormous amount of energy and materials. Furthermore, at a time when consumers are increasingly vocal in their criticism of Direct Marketing, we should all be making an effort to ensure that the industry as a whole is doing all that is possible to minimise wastage.

8.10 Responsibilities

The client is responsible for ensuring that:

- A clear written brief is provided for the hierarchy of any Suppression File to be used if this is a requirement.
- Further information requested by the supplier is supplied in a timely fashion.
- Where a data audit (i.e. a sample of file with verification of matching) has been requested, this is signed off promptly. The client should look closely at the suppression match results and surrounding issues to ensure a satisfactory level of accuracy.

The supplier is responsible for ensuring that:

- A clear brief has been received and understood and any special processing requirements have been clarified and agreed.
- Suppression hierarchies are used according to the brief with sample matches supplied if required.
- Any problems with the data received are advised to the client as soon as possible.
- Audit reports are provided showing the progress of records through the process, including how many records have been suppressed and why.
- Any queries are raised with the client as soon as possible.

9.0 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:

- To improve the data used in customer segmentation and targeting, understanding the demographics of the data and building propensity models that indicate the future likelihood to purchase or be receptive to the brand.
- To identify triggers that suggests a change or a future change in purchasing activity (for example, moving house).
- To infill missing variables (e.g. where income is held on some customers but not all).
- 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 (and commercial databases that augment the edited Roll with additional name and address data from various sources).
- Lifestyle databases.
- Pooled databases of clients' trading data.

The advantages of data tagging can be substantial. However, the costs of tagging can also be considerable. It is important to be clear about why external data are needed in order to assess the likely value to be gained.

If the extra data are being obtained largely for targeting, especially for use in statistical models that will determine who will be contacted, it is important to test variables before deciding which ones to buy. For example, which variables give uplift to models and by how much? Ideally, data should be retested every year since customer profiles may change as the business changes.

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.

Careful matching can mitigate the first of these two risks. Matching procedures need to ensure there is minimal possibility that two individuals within a household or company may be confused. Matching at surname and initial may not be sufficient where there is any likelihood of two individuals with the same surname and initial within the same household or company. Where possible, a match will be made or validated 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 are 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 best used for definitive client specific messages, but it often adds value in providing the treatment or tone of the message.

Where modelled data is provided as part of a data tagging exercise, the supplier should be able to say how accurate the modelled data is (e.g. confidence levels giving percentage accuracy for a variable).

The use of a control cell, using a random selection of unenhanced data, will provide a measure of the additional value the tagged data supplies. Testing a double control periodically can provide a good reality check. Taking two separate control cells containing the identical content, it is interesting to see the variance in the performance of two identical communications sent randomly to individuals.

9.1 Responsibilities

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 are 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.

10.0 Sortation and Output

10.1 Sortation for Postal Discount Schemes

Data can be sorted into any sequence requested by a client; however, they can be specifically sorted in a sequence that will facilitate bulk-mailing discounts from postal carriers. There are a number of discount schemes that vary according to the carrier and service being used. The schemes generally provide postage discounts in return for minimising the amount of preparation and sortation work that the postal carrier is required to do itself. These are typically based on sortation into postcodes, but may also require further sortation into zones and formats. Different discount schemes may also require additional information printed on the envelope, such as a selection code and/or zone.

Example:

Mailsort 1400 from Royal Mail is one of the simplest discount schemes and requires a minimum mailing of 4,000 items and a minimum of 90% of the file to be accurately postcoded. Depending on further selections within this service, discounts can typically be between 8% and 30%.

A good bureau should be able to process data to meet the requirements for each of the schemes, including the production of all the required support documentation. The full details of the schemes can be obtained from the relevant postal carrier.

There are 22 licensed postal carriers as of January 2009 and a full list can be found at Postcomm's website <http://www.psc.gov.uk/licensed-postal-operators.html>

Most postal operators do not publish technical details of their sortation and mail presentation requirements on their websites and you will need to contact them directly. The exception is Royal Mail where you can see the requirements for their bulk mail services at www.mailsorttechnical.com

10.2 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.

10.3 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.

10.4 Responsibilities

The client is responsible for ensuring that:

- Data is provided in accordance with the Royal Mails mail processing guide; Know How (the user's manual for Mailsort®, Presstream®, Walksort®, Presstream® Walksort®, Cleanmail®, Royal Mail International Bulk Mail™ and Automated Standard Tariff Large Letter
 - <http://www.royalmail.com/portal/rm/content3?catId=50800710&mediaId=50800713>

The supplier is responsible for ensuring that:

- Data is processed in accordance with the Royal Mails mail processing guide; Know How (the user's manual for Mailsort®, Presstream®, Walksort®, Presstream® Walksort®, Cleanmail®, Royal Mail International Bulk Mail™ and Automated Standard Tariff Large Letter

- <http://www.royalmail.com/portal/rm/content3?catId=50800710&mediaId=50800713>

DATA GLOSSARY

"Data" refers to 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 are structured in such a way that specific information relating to a particular individual is readily accessible).

"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 is, or is to be, processed.

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

"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.

"Personal data" refers to 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 may also be regarded as personal data and are, therefore, covered by these rules.

"Sensitive personal data" means personal data consisting of information as to:

- a) The racial or ethnic origin of the data subject.
- b) His/her political opinions.
- c) His/her religious beliefs or other beliefs of a similar nature.
- d) Whether he/she is a member of a trade union.
- e) His/her physical or mental health or condition.
- f) His/her sexual life
- g) The commission or alleged commission by him/her of any offence.
- h) Any criminal proceedings.

"The Data Protection Principles" are the eight principles contained in the Data Protection Act 1998 (Schedule 1), which prescribe the required conduct for the lawful management of personal data.

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

"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 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" is a person who may become a customer.

"Warm Prospect" is a person with whom a relationship has been established.

"Cold Prospect" is a person with whom no relationship has yet been established.

USEFUL ADDRESSES

DMA (UK) Ltd

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7291 3300
F 020 7323 4165
E dma@dma.org.uk
W www.dma.org.uk

DMA North

One Central Park
Northampton Road
Manchester
M40 5WW
E suzanne.kay@dma.org.uk
W www.north.dma.org.uk

DMA West

The Cube
1 Lower Lamb Street
BRISTOL, BS1 5UD
T 0117 317 8192
E andrew.buffrey@dma.org.uk
W www.west.dma.org.uk

DMA Scotland

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

Information Commissioner

The Information Commissioner's Office
Wycliffe House
Water Lane, Wilmslow
CHESHIRE, SK9 5AF
T (01625) 545745 (enquiries)
T (01625) 545740 (registration)
W www.ico.gov.uk

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

Postal Address
DMA House
70 Margaret Street
LONDON, WIW 8SS

Mailing Preference Service
Registration Line: 0845 703 4599
Office Number: 020 7291 3310
W www.mpsonline.org.uk,

Baby MPS
W: <http://www.mpsonline.org.uk/bmpsrl/>

Telephone Preference Service
Registration Line: 0845 070 0707
Office 020 7291 3320
W: www.tpsonline.org.uk

Corporate Telephone Preference Service
Office: 020 7291 3320
W: <http://www.tpsonline.org.uk/ctps/what/>

Fax Preference Service
Registration Line 0845 070 0702
W: <http://www.tpsonline.org.uk/fps/>

Email Preference Service (run by US DMA – only relevant if sending out unsolicited emails to people ordinarily resident outside EEA)
W: <http://www.dmachoice.org/emps.html>

Royal Mail

W www.royalmail.com
<http://www.royalmail.com/portal/rm/jump2?mediaId=400047&catId=400046> (Bulk mail products including Mailsort)
www.royalmail.com/portal/rm/jump2?catId=400054&mediaId=400084 (Address Management products)

Advertising Standards Authority

Mid City Place
71 High Holborn
London WC1V 6QT
T 020 7492 2222
F 020 7242 8159
W www.asa.org.uk

Committee of Advertising Practice (CAP)

Mid City Place
71 High Holborn
London WC1V 6QT
T 020 7492 2222
F 020 7242 8159
W: www.cap.org.uk

List Warranty Register (LWR)

DMA House
70 Margaret Street
LONDON, WIW 8SS
T 020 7291 3340
F 020 7323 4426
E lwr@dma.org.uk
W <http://www.dma.org.uk/Information/ind-ListIntro.asp>

Office for National Statistics

Cardiff Road
Newport
NP10 8XB
T 0845 601 3034
F 0163 365 2747

E info@statistics.gov.uk
W www.statistics.gov.uk

Direct Mail Information Service (DMIS)

Royal Mail
Mail Media Centre
Stukely Street
London WC1V 7AB
T 020 7421 2250
E infobank@royalmail.com
W <http://www.dmis.co.uk/>