Data guide

Contents

Contents

Contents

Data care

Contents

Acknowledgements

The DMA would like to acknowledge the contributions to this guide of the members of the DMA Data Council:

Christine Andrews, DQM Group Limited

Lisa Chittenden, Transactis

Jonathan Clough, Acxiom Ltd

Steven Day, UKChanges

Tim Drye, DataTalk

Rachel Hall, Honda (UK)

Tony Lamb, Royal Mail

Suzanne Lewis, EDMMEDIA

Chris McDonald, Call Credit Group

Introduction

Data and the DMA Code

Data is the cornerstone of one-to-one marketing, an indispensable but fragile resource – so it is in your interests to treat your access to customer data as a privilege, not a right.

Maintaining the highest possible standards of data practice is about much more than mere compliance – rather, it is about delivering one-to-one marketing that is a true *exchange of value* between your company, looking to prosper, and your customer, looking to benefit.

One of the five aspirational principles of the DMA Code covers your approach to data and asks you to:

> **Be diligent with data**
> Treat your customers' data with the utmost care and respect

Handle your customer's data with honesty, fairness, care and respect, putting your customer first, and you can look forward to more rewarding, more sustainable and future-proof marketing success as well as making yours a much better and more valued company.

Data best practice is vital – so you should assign responsibility at board level for understanding, planning, managing and monitoring data practice across your organisation.

Outcomes of data best practice

- **Mutually-beneficial marketing**
  Marketing, at its best, is something that is welcomed and desired – a positive, mutually-rewarding relationship between your businesses and your customer.

  This goal relies on high-quality, well-used data in order to deliver the right service and right marketing messages to the right customer at exactly the right time.

  The better you handle your data, the more successful and valued your business will be.
- **Campaign efficiency**
  Good data will help you to make your one-to-one marketing more cost-effective – avoiding waste and saving money and resources.
- **Effective targeting**
  Use precise data to target good customers more effectively, driving higher relevance and response rates.
- **High conversion and retention**
  Better communication delivers better results – building your conversion, customer relationships, brand reputation, brand relevance and long-term loyalty.
- **Customer goodwill**
  Reduce the chance of annoying your customer with irrelevant or incorrect communications – such as duplicate or mistaken messages, mis-spelt names, ignored preferences or inappropriate information.
- **Stronger industry**
  Well-targeted, well-produced and beneficial one-to-one marketing helps to foster a more positive attitude amongst consumers towards the industry – and your business.
- **Preservation of self-regulation**
  Best practice is a vital condition of our industry self-regulation.

Data fundamentals

Legislation

Data legislation is designed to protect the rights of the consumer and ensure that any personal data held or used is both accurate and up to date.

Data availability and use for marketing is subject to ever-increasing legislative scrutiny – making it absolutely critical to your future business success to remain compliant and future-proof in the way you source and handle consumer data.

Check www.legislation.gov.uk to keep up to date with latest amendments for these and all other legislation.

The Data Protection Act 1998 (DPA)

The DPA is the key legislation governing your one-to-one marketing activity.

It has two main aims:

- To protect the rights of the consumer
- To require that any data you source is necesary, fairly and lawfully collected and is kept accurate and up to date

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR)

PECR adds requirements regarding electronic marketing channels – including telephone, email, mobile and connected devices and fax.

Industry codes

Data compliance is also governed by a number of industry codes.

The key codes are:

The British Code of Advertising, Sales Promotion and Direct Marketing (CAP Code)

The DMA Code

Regulatory organisation

The Information Commissioner's Office (ICO)

The eight principles of data protection

The DPA outlines eight principles to which you must adhere when dealing with consumer data.

As well as ensuring compliance, following these principles will improve both your relationships with your customers and the effectiveness and efficiency of your marketing.

1. **Fair and lawful**
   Customer personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.

2. **Stated purpose**
   Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. **Relevance**
   Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. **Accuracy**
   Personal data shall be accurate and, where necessary, kept up to date.

5. **Time-sensitive**
   Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. **Individual rights**
   Personal data shall be processed in accordance with the rights of data subjects under the DPA.

7. **Security**
   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.

8. **Keep data within EEA**
   Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of consumers in relation to the processing of personal data.

For further details see the ICO's *Guide to the Data Protection Act*:

ico.org.uk/for_organisations/data_protection/the_guide

Your obligations

You currently MUST:

- **Consent**
  Ensure you have appropriate consent before you use any consumer data for marketing purposes.
- **Stated use**
  Only use data for the purpose for which it is provided.
- **Honour customer preferences**
  Honour each customer's data preferences.
- **Accuracy**
  Ensure that any data held is accurate.
- **Up to date**
  Ensure that any data you use for marketing purposes is up to date.
- **Security**
  Ensure appropriate data security.
- **Staff training**
  Train your staff to handle data appropriately.

You currently SHOULD:

- **Opt-in**
  As EU regulation moves towards an opt-in environment, you should already start to look to get explicit opt-in consent from your customer to use their personal data for marketing purposes.
- **Respect**
  Use customer personal data with respect, relevance and sensitivity.
- **Define policies**
  Maintain clear policies and processes.
- **Assign data responsibility**
  Assign clear responsibility for data within your organisation.

Penalties for non-compliance

Any organisation that fails to comply with the DPA leaves itself open to action by the ICO and being fined by the courts.

The ICO has the power under the DPA to issue monetary penalty notices for major breaches of the eight principles of data protection.

The ICO takes a strong stance on ensuring compliance and the courts have fined a number of organisations for breaches of the DPA.

There is also the risk of a private civil action for damages as well as significant reputational damage.

To find out the latest information on penalties and sanctions, including examples of companies that have been penalised, visit:

ico.org.uk

Data acquisition

Data capture strategy

Goal-setting

- **Aim for personalised communications**
  Aim to only collect data that will demonstrably improve your ability to deliver highly personalised, relevant and effective one-to-one communications.
- **Fit data capture goals to marketing strategy**
  Match your data capture to your marketing strategy so that you collect the right information to feed your campaigns.

  Using the correct information will obviously improve the results of your marketing activities and analysis.

Strategy

- **Choose data types appropriate to your task**
  Whatever your task, there are likely to be different data sets that could inform it.

  Understand which data types are most relevant to your specific task – and take into account the nature of your product and customer relationship.

  For example, if you are setting the price of a can of baked beans, you can get enough information from geo-demographic tagging to help you set prices that customers will find appropriate from place to place. You do not need to incur the cost and trouble of asking customers to reveal their household income.

  But if you are a retailer, asking for household income might be valuable to work out your current share of wallet and potential customer value.
- **Plan data as a trade with your customer**
  The time to capture more specific data is usually when you can offer a clear and relevant reward – for example, exchanging your customer's email address for an information download, or collecting their postcode in order to offer a personalised insurance quote.
- **Ask for the bare minimum you need**
  The less information you ask for, the more likely your customer is to share their information. Do not ask for information for the sake of it – any data will cost you money to process and will affect your customer's expectations of you.

Opportunities

- **Plan pro-active collection opportunities**
  Be imaginative about where and when you collect data – do not rely solely on a sign-up webpage.

  Instead, proactively ask your target customers for information at relevant moments – such as in-store, at a relevant event or during targeted marketing activities.
- **Time your request**
  Ask for information at the point at which it is most appropriate.

  For example, you might ask for information whilst your customer is using your product; or schedule further information gathering for relevant points in your customer lifecycle.
- **Split your data capture into relevant stages**
  You can always ask for further information at more appropriate opportunities, later in your customer lifecycle.

Logistics

- **Record all data clearly, accurately, accessibly and usably**
  Collect data in the right format to save considerable time and expense later down the line.
- **Integrate data capture with your other systems**
  Wherever possible, gather data into your existing CRM or database to increase efficiency and ensure quality.
- **Store permission statement**
  Compliance will continue to get stricter about requiring you to track the data chain right back to the moment of collection – so always append you customer's data with the precise time, location, channel and means of collection, along with the permission statement to which they agreed.

Consent

Gaining consent to use personal data

- **Gain consent before marketing**
  It is extremely advisable to gain clear, positive consent before marketing one-to-one to any consumer.

  Although this is not currently an absolute legal imperative, data protection regulation is currently being revised at EU level and it is very likely that demonstrable opted-in permission will become a legal requirement.
- **Meet your industry code obligations**
  It is your legal obligation under the DPA and the PECR to gain consent – and a condition of all relevant industry codes and standards, including the DMA Code and the CAP Code.
- **Future-proof your right to market one-to-one**
  It is strongly recommended that you treat opt-in as an obligation.

  This is a common-sense practice that will improve the effectiveness and efficiency of your marketing now – and future-proof your database against the likelihood of opt-in becoming a legal imperative.
- **Safeguard against negative customer reaction**
  Your customers are much more aware of privacy and data issues than ever before and are sensitive to the unprecedented volume of marketing messages they receive on a daily basis.

  Avoid negative perception by only marketing one-to-one to customers who know that they have given you their consent to do so.
- **Improve customer relationship**
  More positively, gaining consent is enables you to give your customer one-to-one marketing that offers them a real benefit and positive experience.

  It is common sense that marketing to customers who are happy to receive your messages will be much more effective, efficient and rewarding than if you market to those who do not welcome it.
- **Understand sanctions**
  You can face possible sanctions for marketing one-to-one without proper consent.

  See the *Penalties for non-compliance* section of this guide for more information.

Data acquisition

Obligations to your customer at sign-up

- **Secure opt-in consent for marketing**
  You must explain if your customer's data is to be used for your own marketing or passed to third parties for marketing purposes.

  For digital marketing you must name any third parties and obtain appropriate consent – unless you are using host emailings. See the *Third-party data and consent* section for further details.

- **Identify yourself clearly**
  Openly and obviously identify all organisations involved in collecting, handling and using your customer's data.

  This will help build trust and improve your data collection and quality, as well as being a duty to your customer.

- **Provide 'stated purpose'**
  However you capture data you need to provide your customer with a clear and prominent statement that explains your 'stated purpose' – what data you are collecting and what you intend to use it for.

- **Publish privacy statement**
  See the *Privacy and data protection notices* section of this guide for details.

- **Declare any third-party usage**
  If you intend to host emailings for third parties then you must inform your customer of this at the point of data capture.

Channel-specific consent rules

Email and SMS

Opt-in

'Opt-in' consent is the express permission by a consumer to receive marketing communications.

- **Higher threshold for digital**
  PECR establishes a higher threshold of consent for gathering and using data in electronic/digital channels.

  Be aware of the difference or default to the highest standard of consent across channels.

- **Future-proof your data**
  It is extremely advisable to gain the highest level of consent, clearly recorded against a permission statement, to future-proof your data as robustly as possible – ahead of tighter data protection regulation to come into force in the near future.

Soft opt-in

- **Specific to email and SMS marketing**
  Soft opt-in applies solely to email and SMS marketing and allows you to conduct one-to-one marketing on the basis of opt-out as long as the following criteria have been met:
    - Your customer's data was collected as part of a sales process or negotiations for a sale
    - Your customer was told at the point of collection that you would use their email address or mobile number for marketing purposes
    - Your customer was given a clear and easy opt-out opportunity
    - Your marketing relates to your own similar products and services
    - Your customer is given an easy and free-of-charge unsubscribe option on each subsequent communication
    - The identity of the sender organisation is clearly shown

- **Fundraisers cannot use soft opt-in**
  Charitites can only use soft opt-in for their trading arms, not for fundraising.
- **Get explicit opt-in**
  In most cases, soft opt-in is NOT best practice – it is much better practice and more successful to gain positive consent from each customer before marketing to them on a one-to-one basis.
- **Collect channel-specific opt-ins**
  It is always preferable to collect specific opt-ins for each marketing channel.

Telemarketing

Opt-out

- **Telemarketing is currently opt-out**
  Telemarketing is currently permitted on an opt-out basis.

  However, you should begin to work towards an opt-in approach. There are already 19.8 million phone numbers opted-out via the TPS suppression list (May 2014) and this is increasing by tens of thousands of numbers every month – so opt-out is becoming less sustainable.

Sourcing numbers

- **Number generation is not permitted**
  Under the DMA Code, random or sequential number generation is not permitted.
- **Only use sourced numbers**
  You should always source numbers from a list of live numbers.

TPS compliance

- **Check TPS compliance first**
  You must check any number against TPS before calling it.

  If it is NOT on TPS, you are entitled to call it.

  If it IS on TPS, then you cannot call it – UNLESS it meets the conditions explained in the *Telephone Preference Service (TPS) – Calling your own customers who are registered on TPS* section of this guide.

Consent rules across all channels

The following best practice guidelines apply to ALL one-to-one marketing channels, including email and telemarketing.

Remember that the DPA applies to all marketing channels, whilst PECR applies only to electronic channels.

Opt-out

- **Right to opt-out**
  Consumers have the right to ask your organisation, by writing, to not send them any further one-to-one marketing.

  This prevents you from processing their data again for marketing purposes.
- **Add consumer to in-house suppression list**
  It is key that you continue to hold this data for suppression purposes, to prevent further uses of this data – whether you are contacting prospects or marketing to existing customers.
- **Use most recent instruction**
  In all cases, it is the most recent piece of information or instruction received from your customer that takes priority.

Data acquisition

Stated purpose and permitted purpose

- **Stated purpose**
  You must tell your customer the purposes for which you will be processing their personal information – and give them the appropriate opt-out or opt-in options.
- **Permitted purpose is stated purpose**
  Your permitted purpose is the reason(s) that you state for collecting your customer's data.
- **Do not use data for any other purpose**
  You must only use your customer's data for the purposes you stated to them when the data was collected, as per the second principle of the DPA.
- **Offer opt-out**
  It is a requirement to offer your customer the ability to 'opt-out' of use of their information for marketing purposes.
- **Abide by specific permission**
  In this situation, you MUST ensure that any specific permission provided by your customer is adhered to – they might have opted-in to communications by some channels but not by others.

  Never assume that consent for communication by one channel means consent for any other.
- **Full legal details**
  Please see the second principle of the DPA for full legal details.

Permission statements

- **Template statements**
  Use the DMA opt-in and opt-out statement builder to create statements specific to your needs.

  You can find the template here:

  http://dma.org.uk/uploads/ckeditor/pdfs/DMA_opt-out_and_opt-in_clauses.pdf

Privacy and data protection notices

The disclosures suggested above focus on transparency at the point of data collection regarding your likely future uses of your customer's data. There will doubtless be other data protection-related notices that you will need to provide in a privacy policy as a matter of both law and best practice.

Since it may be inconvenient to provide this more extensive data protection notice at the point of data collection, general data protection best practice allows you to make these other notices elsewhere by way of a clear and easy-to-understand privacy policy.

Strategy

- **Ensure compliance**
  Ensure your privacy policy is compliant with the law and the ICO's *Privacy policy code of practice*.
- **Consult the DMA**
  Data users will need to take guidance on the terms of their own particular privacy policy. DMA members can call the DMA legal team for legal advice.
- **Use privacy statement as a relationship opportunity**
  Far from treating your privacy statement as a long passage of impenetrable legal jargon, use it as an opportunity to impress your customer that your attitudes towards privacy align with theirs.

  A good privacy statement should be a positive agreement – a chance to build trust and brand reputation early on in your one-to-one marketing relationship with each individual customer.

- **Encourage customer to read and understand it**
  You should not have anything to hide – so encourage your customer to take a minute to check your privacy policy and agree with it.

  Remember that your privacy policy is another brand touchpoint and can be as influential as any other piece of communication you publish.

- **Make it plain and simple to understand**
  Use simple, plain, honest language. Simplify legal clauses to make the sense of them clear to understand.

- **Include link to privacy policy at sign-up**
  You must include a privacy policy whenever you ask your customer for their personal information.

  Since it may well be impractical to include this full policy on a mobile communication, it is permitted to include a link to it from your communication.

- **Make it prominent**
  Make your privacy policy accessible in one click by way of a prominently flagged link above your submit button.

  Do not put this link amongst various other general links to terms and conditions, or in a sidebar, or only visible after scrolling to the bottom of your web page.

- **Link from each communication**
  Your privacy policy should also be clearly accessible via a link from every communication.

- **Optimise for devices**
  Optimise your privacy policy for readability on all devices that your customer is likely to use.

- **Attach to offline data capture points**
  If you collect data offline, your privacy policy should be set out, as a matter of best practice, in full and attached to the material – such as an application form – used to collect the data.

Content

- **Make it layered**
  If your customer agrees to a long, impenetrable privacy policy that they probably have not actually read or understood, it is questionable whether their consent can truly be considered valid.

  Therefore you should write your privacy policy in three layers:

  1. **Summary of key points**
     Summarise your key points and policies to be understood at a glance.

     Ensure this is easy to digest on mobile devices, where small print is even less legible.

  2. **Expanded explanation**
     Expand points for those who are interested to understand at a deeper level.

  3. **Full technical detail**
     Make a full, technical version available for formal situations and legal compliance.

- **Make it comprehensive**
  Your privacy policy should set out your complete policy with regard to personal data – and be consistenly applied throughout your organisation and across all data types.

- **Tailor privacy policy appropriately**
  Write a privacy policy that is specific and relevant to your own organisation, industry, customer expectations and your intended data usage.

- **Privacy policy template**
  Key points you should include are:

1. **Details of data collector**
   Name of the company collecting the personal information and a little information about them.

   Your customer is more likely to give you their information if they know about your business and its aims.

2. **DPA compliance**
   Include a statement that your company complies with the DPA.

3. **What personal information you wish to collect and store**
   State what information you will ask for – such as your customer's name, telephone number, email address and so on.

4. **Information usage**
   Explain how you intend to use your customer's information – for example, to process orders, deal with enquiries and/or send marketing updates on products and services.

5. **Whether the information will be used for marketing**
   If you intend to use your customer's details to market to them, provide an explanation of this and explain clearly to your customer how they can opt out.

   Repeat this explanation at your customer's point of sign-up and subsequently.

   If your customer's information might be passed to third parties, you must explain this as well and obtain specific positive consent for this data use.

6. **Explain Subject Access Requests**
   Inform your customer about their right, via making a Subject Access Request, to see any information that you hold on them.

   Explain how they can get a copy of their information from your organisation and how they can correct any errors.

   You may charge an admin fee of up to £10 to your customer for the provision of this information. If you intend to charge, state what you will charge.

7. **Cookies and tracking usage**
   If you use cookies or other tracking methods on your website, app or any other platform, list their purposes and explain how these work.

   You should explain how your customer can object to this and the consequences of objecting – for example, that they may not be able to access certain features or pages on your website.

8. **Third-party websites**
   If your website has links to third-party websites, include a statement that your policy will not apply to those sites that are beyond your control.

   Advise your customer to check the privacy policies of other websites before they share any information.

9. **Changes to the privacy policy**
   State that your policy is regularly reviewed and will be updated from time to time, as appropriate.

   Make sure that you do keep your privacy and data protection policies up to date as regulations continue to change.

10. **Contact details**
    Provide monitored email and postal addresses to which your customer can contact your company.

Cookies & similar technologies

Definition of cookies

Cookies are files that a website puts on your computer when you visit it.

These files are used for a variety of purposes – from identifying a specific computer in order to recall passwords, previous on-site preferences and so on, to collecting data about your browsing behaviour.

Cookies allow you to:

- Improve customer experience
- Gain vital business insight and information
- Gain usable data

Cookie law

Indirect data capture via cookies must take account of data protection regulation.

It is now the law that you must obtain your site visitor's consent in order to place cookies on their computer – and there are various subtleties around how you ask for this and how to implement it.

- **Take a pan-European approach**
  It is likely, or at least possible, that your website will receive visits from outside the UK.

  Different countries have different cookie laws, even within the EU – so get expert advice to ensure that you follow a cookie policy that is compliant for ALL your users.

  Cookiepedia.co.uk is a not-for-profit service that will identify any cookies you have running on your site and can help you understand how to be compliant across relevant countries.

Cookie stakeholders

- **Assign board-level responsibility**
  Assign someone at board level to ensure your cookie management compliant and right for your business needs.
- **Allocate budget and resource**
  You will need to plan resource to handle and maintain cookies as an ongoing compliance activity.
- **Give strong support to your IT team or webmanagers**
  Your IT team or web managers will be key to your understanding, implementation and compliance around cookies.

  Give them the right support to be able to make sure your cookies are providing you with the right, valuable business information as well as improving your customer's experience.
- **Ensure relevant staff are fully aware**
  Make sure that any staff who might be impacted are fully aware of cookie compliance.

  This could include:

  - Technical help desk
  - Public relations team
  - Call centre staff
  - Marketing team
  - Your board!

Checking cookie compliance

1. **Identify the cookies you use**
   Identify all your websites, apps and other places where cookies might be used.

   There are now many third parties who can provide you with an efficient cookie-auditing service, as well as end-to-end solutions.

2. **Assess your cookies against an 'intrusiveness scale'**
   Either develop your own scale or use an industry standard such as the International Chamber of Commerce (ICC).

3. **Categorise each cookie**
   Identify the cookies you are using according to type:
   - Strictly necessary
   - Performance-related
   - Functionality
   - Targeting

4. **Do cookie housekeeping**
   This is also a good opportunity to identify and cookies that are no longer required.

5. **Check cookies maintained by suppliers**
   Do not forget to collaborate with any suppliers who are providing web services, emails, apps or other platforms that use cookies on your behalf.
   - Make sure they are handling cookies in a fully compliant manner, consistent with your own cookie policy.
   - Consider including cookie-handling policies within your supplier contracts.

Methods of gaining cookie consent

Decide how you will obtain consent from users of your site(s) to use cookies.

- **Methods include:**
  - Pop-up boxes
  - Splash pages
  - Landing pages
  - Homepage headers
  - Banners
  - Scrolling text
  - Tick boxes
- **Develop and test your solution**
  Research different methods to judge which might make the most positive, constructive contribution to your customer's experience.
  - Make no assumptions – cookie notification is still a relatively new practice, so be open to new and better ideas
  - Test the end-to-end user experience before launch
  - Be prepared to continually test and learn to improve how you manage this compliance requirement
  - Use language that is appropriate and easy to understand for your audience

- **Terms and conditions**
  Provide a clear link from your website to your cookie terms and conditions.
- **Implied consent**
  As defined by the ICO:
    - Implied consent is a valid form of consent and can be used in the context of compliance with the revised rules on cookies.
    - If you are relying on implied consent you need to be satisfied that your users understand that their actions will result in cookies being set. Without this understanding you do not have their informed consent.
    - You should not rely on the fact that users might have read a privacy policy that is perhaps hard to find or difficult to understand.
    - In some circumstances, for example where you are collecting sensitive personal data such as health information, you might feel that explicit consent is more appropriate.

Cookie maintenance

- **Define maintenance process**
  It is essential that you keep effective control of your organisation's use of cookies to ensure ongoing compliance.

  An agreed policy to manage this regulation is likely to become a key part of managing risk and compliance for your organisation.
- **Listen to user feedback**
  Once you go live, be alert for customer feedback – this may well help you create a more engaging user experience and a more effective site.

Cookie policy

- **Key policy points**
  Alongside your consent mechanism, you will need to provide your customer with easy access to your cookie policy that explains:
    - What cookies/equivalent technologies are in use
    - What these are doing
    - How your user can both provide and withdraw consent
- **Use industry definitions**
  If appropriate, use industry defined descriptions for key terms. Use the ICC's definitions or consult your legal/ compliance advisors.
- **Make cookies appropriate to audience**
  Keep the profile of your site users in mind when updating your policy – for example, will children be using your site?

Further advice

As well as doing your own research to find out how other organisations are innovating cookies, you can talk to a number of authorities for legal or practical advice.

These include:

The ICC

The ICO

The DMA

Data sources

Data capture forms

To design a form that captures good quality, easy-to-process data, consider the following tips:

- **Consider output**
  Design your data capture to suit its ultimate use.

  For example, any information that your customer will see – such as their name or address – will need to reflect their preferred title, spelling, capitalisation, house name and so on; whereas data that you only intend to use internally to inform your targeting can be recorded in the format that best suits your data processing needs.

- **Provide boxes**
  Clear boxes for different fields – such as the lines of an address, or first name and surname – will improve the quality and accuracy of the data you collect from your customer compared to free-form text boxes.

- **Use blocks or 'tiger teeth'**
  Use blocks or 'tiger teeth' to denominate spacing for characters.

  This will minimise the problems of data being entered in different, poor quality or joined-up handwriting, or in different ink colours, and will improve legibility.

- **Provide sufficient space**
  Provide appropriate space for each data element required – not too short, but not confusingly long.

- **Prompt for essential data elements**
  Whatever the medium, design your data capture form to highlight essential information and clearly prescribe the format in which you want your customer to enter their information.

- **Pre-populate data where appropriate**
  To make your customer's life easier and increase your data capture rate, pre-populate your form with any information you already know about your customer.

  For example, if you are asking for further information from a customer who has made an initial enquiry about your product, or is already an existing customer, then do not ask them to fill in details such as their name or contact details again – load them into your digital form or print them onto your paper one.

- **Allow more space for business details**
  Job titles, departments and business addresses typically require more fields and more space than personal information.

- **Leave plenty of space for name and address**
  The average UK name and address record is 48 keystrokes long, but can involve up to nine separate lines of information.

- **Do not overlook country**
  Include a separate prompt for country if you are gathering data from multiple countries.

  This will save you from having to assign each response to a country of origin later.

- **Let customer provide preferred elements**
  Whilst you might be able to deliver a communication using only basic information, give your customer the opportunity to record any preferences that matter to them – such as their title or house name.

- **Ensure legibility**
  Do not print text on strong colours (i.e. reversed out of black) or over images as this will make completion and reading harder.

- **Design for OCR data capture**
  Using blocks and plain backgrounds can also allow data from your form or coupon to be captured using automatic optical character recognition (OCR) processes.
- **Always test**
  Test your coupon before signing off by asking colleagues to complete it.

Data capture by telephone

Telephone response gives an ideal opportunity for data capture of name and address as well as other information.

Telephone data collection obligations

- **State purpose**
  Ensure that your customer is told – either via your IVR or live operator call scripts – the purposes for which you will use their personal information.
- **Offer opt-out mechanism**
  Offer your customer a mechanism – either via your IVR or live operator call scripts – to specifically opt-in or opt-out of receiving your marketing.
- **Process all opt-outs**
  Such opt-out or opt-in requests should be processed in accordance with data protection legislation.
- **Offer opt-outs per channel**
  If possible, give your customer the choice to opt-out of or opt-in to receiving your marketing via specific channels.

Live operator calls

- **Ask for key identifying information up front**
  Include an initial request for your customer's postcode in live operator scripts.

  Use computer software to then return your customer's correct postal address from this, allowing your operator to validate it with your caller and add the house number and any preferred address elements.

  This will also reduce the duration of calls.
- **Use closed, not open-ended questions**
  Be careful when asking open-ended questions as these can extend your call times and can be difficult to analyse.

  Instead, use Yes/No questions, banded information or multi-choice responses as these are quicker to capture and easier to analyse.

Automated call handling mechanisms

To support best practice in data capture, telephone response mechanisms should follow the following guidelines:

- **Do not rush your customer**
  Allow your customer to provide information at their own speed where automated call handling/interactive voice response (ACH/IVR) is being used.
- **Prompt for key elements**
  Your system should prompt for name and address elements – including a double check for key elements, such as postcode.

- **Prompt to spell out difficult words**
  Include a prompt for your customer to spell difficult words to facilitate transcription, unless these are covered by reference to PAF.

Find out more about telemarketing best practice

For more information on telemarketing, see the *Telemarketing guide*.

Asking consumers to refer friends and family

- **Be fair and honest**
  As ever, the key principle is to be fair and honest in the way you ask your customer to share contact details of their friends or family with you.
- **Remember legal obligations**
  You must abide by the same legal obligations when gathering or using referred contact details, just as you would when gathering information directly.
- **Be careful about incentivising referrals**
  You should be very careful about offering incentives to your customer in exchange for another consumer's personal information. An incentivised customer is more likely to act out of self-interest and pass you contacts who have not given their clear, positive, properly informed consent.
- **Encourage the referal to contact you directly**
  Rather than asking your customer to pass you contact details for their friends or family, you are more likely to get good quality, high-value contacts if the friends or family are encouraged to engage with you directly.

  If you wish to incentivise your data-gathering, offer the main incentive to the customer whose details you wish to collect.
- **Be able to show record of consent**
  If you cannot demonstrate your customer's positive consent, with a place, time, date and permission statement, the consent is probably not sufficient.
- **Provide privacy notice**
  Once any customer has engaged with you, do not forget to present them with your appropriate privacy notices at the point of sign-up.

Third-party data and consent

Key issues

- **Consent**
  At best, it can be hard to prove positive consent from the consumers listed in bought or rented data – especially consent to receive marketing from your particular brand, via the channels you wish to use – and you run the risk of upsetting the very customer you wish to sell to.

- **Quality**
  Different third-party data lists will have been compiled from many different sources – not all of them compliant with the DPA.

  These lists are likely to include data that has not been freely, knowingly given by consumers and will be a very bad investment for you in terms of quality of leads as well as non-compliance.

- **Accuracy**
  Bought lists naturally differ in terms of accuracy and recency, dependent on the efforts of the list broker to maintain correct records and the difficulties of updating information when they (and you) have no direct relationship with the customers listed.

  It is also much harder for you to check the quality of third-party data.

- **Responsibility**
  Do strict due diligence on any data supplier to satisfy yourself that using their data will not put you in breach of the DPA and PECR and leave you open to penalties.

Using third-party data

- **Define objective**
  Data purchasing decisions should not be price-led. Have a clear objective and measure your success against this – or use a simple return on investment model. Just because something is really cheap does not mean it is a good idea.

- **Check opt-in**
  Ensure you know who owns the data and how the consumers have given their consent.

  Ask to see the opt-in statements.

- **Control segmentation**
  Be in control of the data selections being used. You want to avoid any negative feedback and association at all cost, so targeting and selections are as crucial as the message you are sending.

- **Test third-party data**
  Monitor responses from third-party data separately to your existing database so that you can measure its effectiveness.

Third-party lead generation

- **Clarify opt-ins**
  When undertaking any data capture on third-party sites, ensure all opt-ins are very clear and ask to see all of the websites and places where the data will be collected.

- **Check sign-up process**
  Go through the process yourself to check that it is clear to your customer what they are signing up for – and that they are not being forced into receiving marketing communications.

- **Tailor your emails**
  Make sure you have an email communication strategy specifically targeted to these customers so that they have a clear idea of why they are receiving information and what the benefit is to them.

  Monitor response from third-party customers separate to your in-house lists so that you can measure the effectiveness and ROI of third-party data from different sources.

Tackling the data chain

If you are using bought or rented data, take steps to check the provenance of the data before you procure it.

This is because data can end up being passed on from one company to the next, sometimes many times – with major implications for compliance and quality.

The risks of a long data chain are:

- **Poor compliance**
  Even with the best of intentions, data that is passed through multiple companies will deteriorate in accuracy, recency and quality as it is processed and re-processed.
- **Cannot be kept up to date**
  Only the initial data collector is close enough to the listed consumers to be able to viably and reliably update their records as consumers' circumstances change.
- **Poor quality**
  Remember that data will inevitably start to decay as soon as it is collected – and that data with a significant chain, or that is no longer maintained by the original data collector, is likely to be riddled with unusable or non-compliant records and is therefore a poor (or even risky) investment for you.
- **Irrelevance to consumers**
  Consumers are increasingly likely to ask questions or be annoyed by one-to-one marketing from brands that they have not signed up for or do not even recognise.

  You should seriously question the value and consequences of contacting any consumer unless you know where their information was captured and are completely confident that they have consented to receive one-to-one marketing from you and will react positively to it.

Sharing consumer data with third-parties

If you might share your customer's data with any third party, you must make this absolutely explicit at their point of sign-up and secure positive consent for this on an opt-in, not opt-out basis.

It is necessary for anyone using your customer data to have a copy of this positive consent, along with the associated permission statement, and to ensure that all usage adheres to the scope of this consent.

Buying, selling and renting data

Data should be rented rather than bought and sold. This is to ensure that list owners are able to meet their obligations to the consumer, made at the point of collection, with regards to how that data is used and maintained.

There is a commercial benefit to renting rather than buying data – as the list owner is able to keep customer records and permissions up to date and the data more valuable as a result.

Renting data is heavily subject to the DPA and PECR – as well as various industry codes such as the DMA Code and the CAP Code.

You will ultimately be held to account by the ICO so must understand and abide by their rules on this issue, which are:

Selling a marketing list

157 Organisations must act fairly and lawfully when selling a marketing list. If an organisation obtained details from individuals with the intention of selling them on, it must have made it clear that their details would be passed on to third parties for marketing purposes and obtained their consent for this. It is good practice to specifically name (or at least give a clear description of) the third parties to whom details may be sold. See the section above on what counts as consent.

158 Anyone selling a list should understand that the rules on electronic marketing are stricter than for more traditional marketing methods, and that they cannot take a one-size-fits- all approach to consent or the sale of marketing lists. A list with general consent to third party marketing may be enough for mail marketing, but is unlikely to cover calls, texts or emails. Call lists must be screened against the TPS, and third-party lists can only be used for text or email marketing in limited circumstances.

159 A buyer will only be able to send marketing texts or emails, or make automated calls, to people on the list if they gave specific consent. Indirect consent – that is, consent given to someone other than the organisation doing the marketing – will not always be enough for this, which means that some marketing lists will be of limited value to buyers wanting to carry out text, email or automated call campaigns. See the section above for more information about the limitations of indirect (third-party) consent.

160 An organisation wanting to sell a marketing list for use in text, email or automated call campaigns will therefore need to keep clear records showing when and how consent was obtained, by whom, and exactly what the individual was told (including copies of privacy notices), so that it can give proper assurances to buyers. Organisations must not claim to sell a marketing list with consent for texts, emails or automated calls if it does not have clear records. We consider it would be unfair and in breach of the DPA to sell a list without keeping clear records of consent, as it is likely to result in individuals receiving non-compliant marketing.

161 An organisation wanting to sell a marketing list for use in telephone campaigns should also make clear whether it has pre-screened the list against the TPS register, and if so on what date it was last screened.

162 Note that it is a criminal offence under section 55 of the DPA to sell or offer to sell a marketing list if any of the customer details were knowingly or recklessly obtained from another data controller without its consent.

163 Although an organisation will usually need an individual's consent to sell their details on for marketing purposes, if a business is insolvent, or being closed down or sold, its customer database can be sold on without prior consent. However, the seller must make sure the buyer understands that they can only use the information for the same purpose for which it was collected by the original business. Any use of the information should be within the reasonable expectations of the individuals concerned. So, when a database is sold, its use should stay the same or similar. For example, if the database contains information obtained for insurance, the database should only be sold to another insurance-based business providing similar insurance

products. Selling it to a business for a different use is likely to be incompatible with the original purpose, and likely to go beyond the expectations of the individuals. If the buyer does want to use the information for a new purpose, they will have to get consent from the individuals concerned.

Buying a marketing list

164 Organisations buying or renting a marketing list from a list broker or other third party must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

165 Organisations should take extra care if using a bought-in list to send marketing texts, emails or automated calls. They must have very specific consent for this type of marketing, and indirect consent (ie consent originally given to another organisation) will not always be enough – see the section above on indirect (third-party) consent. Remember also that the 'soft opt-in' exception for email or text marketing cannot apply to contacts on a bought-in list.

166 Organisations must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence, to demonstrate consent if challenged. Organisations seeking to rely on consent must ensure that consent was validly obtained, that it was reasonably recent, and that it clearly extended to them specifically or to organisations fitting their description.

167 Reasonable due diligence might include checking the following:

- Who compiled the list? When? Has it been amended or updated since then?
- When was consent obtained?
- Who obtained it and in what context?
- What method was used – eg was it opt-in or opt-out?
- Was the information provided clear and intelligible? How was it provided – eg behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Has the list been screened against the TPS or other relevant preference services? If so, when?
- Has the individual expressed any other preferences – eg regarding marketing calls or mail?
- Has the seller received any complaints?
- Is the seller a member of a professional body or accredited in some way?

168 A reputable list broker should be able to demonstrate that the marketing list for sale or rental is reliable by explaining how it was compiled and providing full details of what individuals consented to, when and how. If the seller cannot provide this information, a buyer should not use the list. It would be prudent for a buyer to have a written contract in place confirming the reliability of the list, as well as making its own checks. The contract should give a buyer reasonable control and audit powers.

169 Once an organisation has bought the list it should make sure it is prepared to deal with any inaccuracies or complaints arising from its use. If it receives complaints from individuals whose details came from a particular source, this would suggest that the source is unreliable and should not be used. A sampling exercise might help to assess how reliable the list actually is. It is also good practice to inform the individual where their

details came from and ask whether they want to withdraw consent from other organisations as well, and if so to inform the source that consent has been withdrawn from all users.

170 The DPA requires that any personal information held should be adequate, relevant and not excessive, and that it should not be kept for longer than necessary. Organisations buying a list should decide how much of the information they actually need to keep. Any unnecessary personal information should be deleted. Personal information should not be held simply on the basis that it might become useful one day.

171 Organisations buying a list should also consider providing their own privacy notice to the individuals concerned as soon as possible, unless it would be disproportionate to do so. See the *Privacy notices code of practice* for more information on when and how to provide a privacy notice. We accept that in practice this is likely to be more difficult for organisations making contact by phone.

172 It is also good practice for organisations using bought-in lists to include the name and contact details of the organisation that provided the person's details in any marketing message.

173 Even if an organisation does not need specific consent for its marketing (eg for calls screened against the TPS list, or for mail marketing), it should still not go beyond what the individuals would reasonably expect. It should only market products or services which are reasonably similar to those which have been promoted to those customers in the past, or which they have a clear reason to expect. Bought-in call lists must always be screened against the TPS. And they should also be screened against the organisation's own in-house suppression (do not call) list, to ensure it doesn't contact anyone who has already said they want to opt out of its marketing.

For the full ICO guidance, download their *Direct marketing guidance* PDF:

ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf

Renting consumer lists and data

The starting point when buying data is to have a clear idea of the type of customer you want to contact. The better you are able to describe this customer, the better able you will be to find the most appropriate source.

You will also need to know what you want to communicate – and when and how you want the activity to take place.

Armed with this information, your data supplier will be in a position to make the most appropriate recommendation for your campaign.

Strategy

- **Choose the right data for your business**
  There are various ways in which you can rent and use data – and because the choice (and associated rules) is so varied, getting it right for your business is critical.
- **Aim for precise targeting**
  Through the extensive number of consumer rental lists and databases available in the UK, it is possible to target individuals with a range of interests and lifestyles via multiple channels.
- **Use data lawfully**
  Using consumer lists for the first time, you will need advice on how to select the correct prospects and also how to respect the customer's rights under all current legislation and regulation – including the DPA and PECR.
- **Use DMA members**
  Using list owners and list brokers who are members of the DMA gives you the reassurance that they operate under the strict DMA Code.

Data acquisition

- **Always do due diligence**
  Whoever you source data from, conduct full due diligence on the data owner or broker.
- **Contact the DMA for further advice**
  If you need further answers or advice about renting consumer lists, members can contact the DMA legal team for further advice.

How lists are compiled

Consumer lists can be developed from different sources:

1. **Compiled from publicly available information**
   Records may be compiled specifically as lists for rental, often from publicly available information.

   This type of list would include details of voters on the edited Electoral Roll (which is available to organisations for marketing), supplemented with data from other sources in order to provide as broad a coverage of the UK consumer base as possible.

2. **Compiled from consumer responses**
   Data may be generated in response to an advertising or one-to-one marketing campaign, questionnaires or online/website activity.

   Response lists include buyers or enquirers about products from off-the-page advertisements or advertising mail promotions, as well as competition entrants and visitors to specific cultural events or consumer exhibitions.

3. **Compiled using specific opt-ins**
   There are lists available of consumers who have specifically requested or opted-in to receive information.

   This is often referred to 'lead generation' data. In these instances, the consumers have usually completed some form of online survey and requested information about a product or service.

4. **Business lists**
   B2B lists are are most likely to be compiled using data from Companies House.

List owners, brokers and managers

- **List owners**
  List owners are the generators of lists, either specifically for rental or as a by-product of their main business.
- **List managers**
  List managers take on the job of selling data lists on behalf of a list owner.

  They are remunerated by the list owner on a commission basis according to the number of names they sell.
- **List brokers**
  List brokers buy lists on behalf of clients, much like other media buyers.

  They are a source of impartial advice on data lists as they receive similar commissions from all list owners.
- **End user**
  The organisation using the list for marketing purposes.

  It is not uncommon for the end user to deal directly with the list manager or owner.
- **Data processors**
  Data processors or data bureaux manage the merge-purge process to de-duplicate lists before use and are usually appointed by the end user.

  It is not uncommon for end users to process their data in-house.

Data acquisition

Datacards

- **Ask for datacard**
  Apart from the general information about the origin of the list – which may be in brochures, on the company website or other advertising literature – ask for a datacard on the lists you are considering renting.

  The datacard is similar to an advertising rate card.

  It will probably contain the following information:

    - Source/profile of the list
    - Number of names available
    - Number of names available broken down by key selections
    - Production formats
    - Update method and frequency for the list
    - Price per name or per thousand names
    - Price per selection
    - Minimum order quantity or price
    - Type of selections available
    - Delivery time
    - Address formats/postcoding/email/telephone numbers/mailsort
    - When the datacard was last updated
    - Whether or not the list has been cleaned against the appropriate preference service suppression file
    - Governance on use – how data has been collected and how it can be used

List pricing

Pricing usually has two elements:

- **Base price**
    - Large lists are typically priced per thousand
    - Small lists may have a one-off price for use of all the names
- **Charges for selection and format**
  In addition to the base price, there will usually be further charges for each selection and occasionally for the output format you require.
- **Delivery might be charged**
  Delivery may also be charged extra – though this is less common.
- **Minimum order**
  Remember there will usually be a minimum order quantity or price to consider.
- **Buying on licence**
  Very large data purchases can be made on licence – which will give you access to files for multiple use.

  Prices vary significantly depending on the type of data you are purchasing, but a licence can often be a more cost-effective option.

- **Lead generation**
  Lead generation is more commonly charged at a cost per lead supplied.

  This can range from pence to pounds depending on the type of data required.

- **Cost per response**
  Occasionally, some suppliers of this data will enter into 'cost per response' agreements – which enable you to share the risk (and reward) of a campaign with a supplier.

- **Duplicates**
  There are various methods of compensating you for duplicates when multiple list sources are being used.

Negotiating data purchase

- **Understand different arrangements**
  There are different data purchase arrangements available.

- **Negotiate best arrangement**
  Use you own commercial judgement to identify and negotiate the most appropriate arrangement for your circumstances.

The main methods are:

Net name agreements

Net name agreements base cost on a specific net name percentage deal.**Example 1:**
A typical data rental plan (estimated de-dupe loss set at 15%)

Data source	Order volume	Estimated data volume	Base rental per '000	Run-on per '000	Gross per '000	% net agreed	Net cost
List A	20,000	17,000	£100	£10	£2,000	85%	£1,730
List B	20,000	17,000	£100	£10	£2,000	90%	£1,820
List C	19,000	16,150	£100	£10	£1,900	100%	£1,900
	59,000	50,150			£5,900		£5,450

Oversupply of data

Instead of negotiating a specified percentage net deal, the estimated duplication loss is used to agree an oversupply of data for the equivalent volume.

If data loss is less than the agreed percentage, your data owner may look to reconcile the difference.

- **Example:**

Estimated de-dupe loss	Required order volume	Base cost per '000	Volume delivered	Selection cost per '000	Run-on per '000	% net agreed	Net cost
15% = 2,550 records	17,000	£100 = £1,700	19,550	£0	£10 = £25.50	100%	 = £1,725.50

Data acquisition

Volume-based

- **Economies of scale**
  Quite simply this method works on 'economy of scale' principles – the more you buy, the more you save.

  However, you should be aware that your discount will vary from list to list and will ultimately come down to individual negotiations between seller and buyer.

- **Quick and simple pricing**
  In essence this method seeks to agree a volume-based discount without any net name agreements and thus dispense with the need to raise credit requests or post de-dupe reconciliation – you simply agree a cost-per-thousand and buy the volume you require.

  Volume discount pricing methods are straightforward in that they are not laden with administration – back and forth with credit requests, de-dupe reports and so on.

  For many, this simplistic method is popular.

  However it has its pitfalls as no science or logic intervenes – so you could agree a good deal now only to find out that later, after a de-dupe, you are actually worse off than you first thought.

  It is worth pointing out that these individual negotiations could lead to advantage or disadvantage on either side.

- **No industry standard pricing**
  Also be aware that there is no industry standard on volume discounts and pricing structure – if there were, it would be against the law.

  Expect variations from company to company.

- **Calculate margin for error**
  Whilst this approach is quick and less complex, it is important to ensure that the estimated loss has been calculated accurately otherwise one party could end up losing out.

  For example, should more than 15% be lost in the below example then the end user will have paid more than necessary for the data eventually used.

- **Example:**

Order volume	Estimated de-dupe loss	Negotiated volume	Volume delivered	Base cost per '000	Selection cost per '000	Run-on per '000	% net agreed	Net cost
20,000	15% 3,000 records	17,000	20,000	£100	£0	£0	100%	 = £1,700

Volume discount matrices

- **Work out your volume discount matrix**
  As either a data buyer or data seller it is possible for you to work out a matrix for volume discounts, in advance of buying or selling data, to act as a guideline for you and the other party during negotiation.

  The advantages of preparing your own matrix in advance are that you can work out your cost structure and the areas where you can gain and concede ground.

- **Best for large volumes**
  Volume discounts, by their nature, obviously benefit both sides when larger volumes are being traded and may not be the best method if dealing in smaller volumes.

However, it is entirely up to the buyer and seller to agree a deal they are both comfortable with.

Again, the massive benefit of volume discounts centres almost entirely in the administration of data sales and the clear understanding of the financial position once a deal has been agreed.

This means that for many buyers and sellers, volume discount is a more preferable option than other data trading methods.

- **Example matrix for volume discounts**

Order volume	Discount
0 - 20,000	0%
20,001 - 40,000	10%
40,001 - 60,000	15%
60,001 - 80,000	20%
80,001 - 100,000	25%
100,001 - 120,000	30%
120,001 - 150,000	40%
150,001 - 200,000	50%
200,001 +	65%

Multi-usage and data licence

- **Aim to reduce data costs for multiple uses**
  Multi-use or data licensing is a way of buying data and reducing wastage on list costs, dependant on the number of times you wish to use the data in an agreed time period.
- **Try to negotiate re-mail rate**
  The more times you use the same list or database outside of such an agreement, the higher the cost will be as you are likely to be paying full rate per transaction unless a re-mail rate can be negotiated.

  Most list owners will typically honour a multi-use or data-licence agreement as long as mutually acceptable rates and terms for usage can be agreed on.
- **Consider mixed pricing models**
  Considerations for rates include the number of times you are likely to use the names within the period.

  If you are only going to contact the customers twice, then it may be wise to negotiate a fixed cost per thousand for the first contact and then a reduced rate for a follow-up.

  For example, if you agree to a first stage contact at £100 per thousand base rental, your follow-up rate could be fixed at 75% of the agreed first mailing rate – ie. £75 per thousand base rental.
- **Consider reduced-rate pre- and post-mailers**
  Some list owners may offer a reduced rate for a pre-mailer followed by the full rate for your actual campaign.

  Additionally, some list owners could also offer a price incentive for a post-mailing.
- **Re-supply of data**
  If you require a re-supply of the data before any subsequent contact, the list owner may require additional payment for selection costs and/or data processing costs.

  Check your agreement in advance of the transaction.

- **Consider data licence arrangement**
  If you are planning on contacting the list more than twice, it might be more practical to agree a data licence fee.

  These periods are usually for a maximum of one year – although with the right data hygiene procedures, you can extend its lifetime for as long as you have the appropriate agreement.

- **Take data cleaning into account**
  The cleanliness of your data is very important when licensing or leasing data and is usually a factor to consider when negotiating the price.

- **Summary of considerations:**
  In summary, terms for consideration when negotiating are:
    - Duration of the agreement
    - Number of times data will be used within the period
    - Permitted purposes and media channels the data will be used for
    - Whether the data is to be overlaid with other variables – either from the same list owner or another source
    - Data cleaning – whether suppression files or a total refresh of the data will be supplied

Reporting on list usage

- **Produce a de-dupe report**
  In order to prove usage under a net names agreement or oversupply agreement you will need to produce a report showing how much data has been lost during the merge-purge de-duplication process.

- **Report within three months**
  The typical timeframe for producing such a report is three months of supply – although you need to check the terms of your specific data order with your supplier.

  If you miss the deadline then you are unlikely to be able to claim your credit – unless you have prior agreement with the data supplier.

  Before entering into a rental agreement, check the terms so that you understand what your obligations are – they will often vary from supplier to supplier.

- **Keep audit trail**
  Net names rebates are affected by where in a hierarchy the list is introduced for de-duplication – the lower in the hierarchy, the higher the number of duplicates that are likely to be produced.

  To maintain trust in this process and in negotiation with your list supplier, ensure that your data processor maintains a complete audit trail and provides it if required.

- **Further guidance on hierarchies**
  See the *Hierarchies* section of the *Advertising mail* guide for more information on creating de-dupe hierarchies.

- **Net name agreements cover duplicates against in-house data**
  It is worth noting that net name agreements are negotiated to ensure you do not pay for duplicates against your own in-house data – or against other external data sources that you have already purchased and processed.

- **Suppressed records NOT included**
  Bad addresses, preference service matches, internal duplicates and data lost when screening against industry suppression files are a separate issue and not usually included in your net name agreement.

- **Check your terms of use**
  In all cases it is advisable for you to check the individual terms of use and to negotiate or specify your particular requirements in advance of making your purchase.

- **Example de-dupe report**

Data Crunching Co.

De-duplication report

Number	AB1234	**Data user**	Books4Me		
Date	38,473	**Mail date**	May-14		
Campaign	Summer mailing				

Supplier	List name	Selections	Order volume	Volume received	Mailed volume	Agreed nets	Actual nets	Names lost
Lists Direct	Over You	0-6 month recency, multi buyers	189,000	189,000	100,000	45%	47%	89,000
	Hill Hikers	Active subscribers	50,000	50,000	25,000	50%	50%	25,000
	Traditional Needlework	0-12 month recency, aged 50+	200,000	200,000	110,000	60%	45%	90,000
Supplier total			**439,000**	**439,000**	**235,000**			**204,000**

Conditions of use for bought data

Permitted use

- **Submit sample creative**
  Before a list is released you will be required to submit a sample creative mailing piece, sample telephone script or copy of the proposed email to the list owner for approval.
- **This is your approved collateral**
  You may only send the approved piece to the list unless otherwise agreed with the owner.
- **Ensure compliance of collateral**
  You will need to ensure that the piece conforms to the DMA Code and the CAP Code, as well as ensuring that it is legal.

Ownership

- **One-time use**
  Most lists are made available for one-time contact only.

  Additional uses, including follow-ups, have to be agreed with the list owner.
- **Bought or licensed lists can be used repeatedly**
  Some lists are made available for multiple usage and are sold outright or on licence.
- **List owner retains data ownership**
  In all cases the list owner retains the copyright of the list and is the legal owner of the data and you will require permission to load it onto your own database.
- **Lists usage will be tracked**
  All lists include seed names which are dummy records addressed to the list owner or his agent.

  Unauthorised usage of lists will, therefore, be detected by the list owner – and will be subject to further charges and possible legal action.

Data acquisition

Ownership of respondents' data

- **You own responders**
  If a consumer responds to your communication (other than to make a complaint or to unsubscribe) then you can add their record to your own database and are free to continue to contact them without any further charge.

  This is subject to the proviso that the consumer has been given the appropriate data protection notices and opt-out opportunities.

- **You do not own non-responders**
  Non-responders remain the property of the list owner – you may only re-contact them with the owner's permission.

Seed names

Data owners often seed their lists with certain records, often fictitious, in order to monitor the data usage process or unauthorised use of the list.

The number of seeds added will depend on the size of your list, but check this in advance and clarify in the terms and conditions of use.

Quality and response guarantees

- **Do not expect guaranteed response rate**
  It is impossible to predict response rates accurately on any list as it is very much dependent on your marketing offer, your creative treatment and the timing of your communication.

  You will not receive guarantees of response from list suppliers, although they will be able to tell you in broad terms if the list has worked for similar offers in the past.

- **Ask for quality guarantees**
  Some list owners offer guarantees on deliverability and quality of addressing.

- **Explore 'risk reward' deals**
  Some suppliers will also consider 'risk reward' deals where you pay based on response rates.

Returns

- **Expect some returns**
  No list will be 100% accurate and you should expect some returns or gone-aways.

- **Put a returns-handling system in place**
  It is advisable to have a system in place to facilitate handling of gone-aways and complaints.

- **Return gone-aways to list owner**
  The DMA Code and the CAP Code require you to return all gone-aways to your list owner promptly for removal.

- **Gone-away return schemes**
  List owners operate different schemes to incentivise the return of gone-aways and some offer a credit for returns over a certain percentage.

Third-party data compliance

List rental and the DMA Code

The DMA Code contains rules for members which have to be adhered to by list suppliers, processors and users.

You should be familiar with your responsibilities under the Code, as well as those of owners, brokers and managers.

List owner obligations under DPA

- **Register with ICO**
  All list owners in the UK must go through the process of notification/registration with the ICO and must collect data both fairly and lawfully.
- **Check customer consent**
  Check the details of customer registration and notification and ensure that the customer has been offered an opt-out (for postal or telemarketing data) or that the data has been fairly obtained from publicly available sources.
- **Gain positive consent for email data**
  Email data has more stringent rules applied and is subject to opt-in for third-party rental.
- **Data owner must send campaign**
  Many prospect email campaigns must be broadcast by the data owner – rather than your own email service provider.
- **Further information**
  Please refer to the *Email marketing guide* for further information about best practice in email marketing.

List user obligations under DPA

- **Register with ICO**
  List users who hold data on consumers (including those at business addresses) are also required to notify/register with the ICO unless they are exempt.
- **Gain professional advice**
  For further information on your obligations under the DPA, or to find out if you are exempt from notification, DMA members can contact the DMA legal team for free advice.

  Alternatively, contact the ICO.

  ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx

List hygiene

- **Screen against preference services**
  It is a legal requirement and your obligation under the DMA Code and CAP Code to screen your lists against the relevent preference services before each time you use them.

  The onus is on you, as the list user, to ensure that your data is correctly screened before use.

  The preference services are TPS, CTPS, MPS, BMPS, FPS and *Your Choice*.

  See the *DMA preference services* section for full information.
- **Use commercial suppression files**
  There are many commercially available suppression files enabling list owners and list users to clean their databases of deceased people, gone-aways and so on.

Many of these files are commercially available and, whilst their use is not compulsory, it is highly advisable that you screen against any appropriate suppression files prior to your campaign to ensure that your data remains accurate and high-value, as well as compliant.

- **Take extra care to screen for deceased people**
  One of the most common causes of complaint against one-to-one marketers comes from relatives of deceased people who are distressed by continuing marketing communications targeted to the deceased.

  Take extra care to screen for deceased people to avoid causing upset and receiving complaints.

Data transfer formats

- **Send data securely**
  You must ensure that lists are transferred securely – using the most up-to-date encryption and strong, unique, regularly changed passwords.
- **Further information**
  For further information, see the *Sharing data* section of this guide.

Data delivery

- **Delivery times**
  Some lists can be supplied very quickly.

  Same-day or overnight delivery is not uncommon, but most will take around 2-4 working days from the point at which the order is approved by the list owner.
- **Use DMA members**
  Most list owners will only allow lists to be delivered to a mailing house or data processor that is a member of the DMA.

Receiving a consumer complaint

You might receive a complaint from a consumer contacted using third-party data.

The action you need to take depends on the type of complaint you have received.

- **Unsubscribe requests**
  For straightforward unsubscribe requests, refer to the *Unsubscribe requests* section.
- **Repeat complaints**
  It might be that you receive a complaint from a consumer who has already unsubscribed from your communications before.

  This indicates that you might not have run your in-house 'do not contact' suppression file against your bought list.

  In this case, you must suppress their data from your own database and inform the list owner to do the same.
- **"How did you get my details?"**
  It is good practice to know and be able to explain to your customer where you got their data from.

  It might be that this will satisfy their need for information – and prevent them from feeling intruded upon by your brand.
- **Subject Access Requests**
  If your customer wants to know what information you hold on them, they can make a Subject Access Request under Section 7 of the DPA.

  See the *Subject Access Request* section of this guide for more details.

Unsubscribe requests

Unsubscribe or 'do not contact' requests

- **Honour consumer's right**
  Consumers have the right, under Section 11 of the DPA, to ask you to stop contacting them for marketing purposes.

  They must give notice of this request in writing.

  However, just as you should be honest and fair in all your business practice, you should honour your customer's intention to unsubscribe even if their request is not in writing – after all, they are hardly likely to be receptive to your future marketing if they have asked you to stop sending it.

- **Identify scope of request**
  Your customer might wish to unsubscribe from all your marketing or just one specific marketing channel.

  If possible, give them this choice.

- **Acknowledge request**
  You should acknowledge this request within a reasonable period of time.

- **Manage customer expectations**
  Manage your customer's expectations by warning that they might continue to receive communications for a certain period of time after being unsubscribed, as you might have further communications already in production that are past the point of recall.

- **Inform about preference services**
  If your customer wishes to unsubscribe from all marketing via a particular channel, direct them to the relevant DMA preference service – TPS, CTPS, MPS, BMPS, FPS and *Your Choice*.

- **Explain data source**
  You should know and be able to explain to your customer where you got their data from.

  It might be that this will satisfy their need for information – or prevent them from feeling intruded on by your brand.

Information requests

Subject Access Request

Section 7 of the DPA gives consumers certain rights in respect of their personal data – including the right to make a Subject Access Request.

- **Provide all information**
  A Subject Access Request requires your data controller to provide your customer with certain specified information and a copy of all personal data you hold on them.

- **Provide within 40 days**
  You must fulfil the request within a maximum of 40 days from the date of receipt of the written request and the payment of the fee, if the fee is charged.

- **Maximum fee**
  The maximum fee you can charge is £10.

Further information

For further information and guidance on using third-party data, the DMA offers a wide range of information, resources and advice, including:

- dma.org.uk
- Channel-specific sections of the DMA Guides
- The DMA Code
- The DMA's guide *Best practice in information security*
- Regular DMA events about data issues
- The DMA legal team

Data care

Data hygiene

Data decay

It is inevitable that data will start to decay as soon as it is gathered.

For example, 1.5 million households – over 10% of the adult population – change address every year in the UK.

And in 2011 alone, nearly 74 million records were suppressed from mailing files – representing 4.3% of all advertising mail. It is estimated that this represents only about 50% of mail that is addressed incorrectly.

(Source: *Data IQ Industry Report – Data Quality Suppression Files*, January 2012, published by DQM Group in partnership with the DMA).

Other data, especially rich data used to profile customers on spending power or buying preferences, is even more sensitive to changes in individuals' circumstances.

Strategy

You need to strategise and resource for data hygiene as a business-critical activity.

One of the principal drivers of one-to-one marketing is to retain existing customers – and you can only do this if you keep their information accurate and up to date.

- **Prioritise your brand reputation**
  All one-to-one marketing is about communication with individuals – so communicating with each customer correctly and accurately is imperative.

  How you communicate with your customer is an indication to them of how you feel about them – so make sure it feels positive and mutually beneficial.

- **Approach as an investment**
  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 – so consider data hygiene costs very much as an investment, not an expense.

- **Plan data hygiene for key points in your customer lifecycle**
  During the course of your customer's relationship with your organisation, it is likely that you will gather a greater wealth of data about them – including more sensitive information, such as date of birth or financial status.

  Implement an appropriate updating cycle to make sure that your data is cleaned at important moments – such as after a purchase or a change of customer status.

- **Conduct data hygiene before campaigns**
  The more accurate your data, the more efficient and effective your campaign will be – so place extra emphasis on cleaning your data before using it to launch a campaign.

Legal obligations

- **Accurate and up-to-date**
  It is a legal requirement under the DPA that "personal data shall be accurate and, where necessary, kept up to date".

- **Necessary**
  You should also conduct data cleaning to remove records that you no longer need – the DPA states that "personal data should be kept for no longer than is necessary".

Data care

Maintaining data hygiene

- **Encourage customers to maintain their own data**
  Digital media also provide an excellent opportunity for your customer to maintain their own data – either through emailing requests to update their records, being asked when calling in or being prompted to go online to change their details.
- **Plan ahead**
  Make sure your data updating facilities are in place and that your team understand the processes and goals in plenty of time before you need to use the finished file.
- **Register unsubscribes promptly**
  Make sure your team are able to quickly and easily register unsubscribe requests – and that your systems update these preferences as promptly as possible.
- **Update all data changes promptly**
  Record changes to any details – such as address, telephone number, job function and so on – within a reasonable period of time.
- **Update master file**
  Transfer data updates to your master file before use.
- **Maintain in-house suppression lists for specific channels**
  Maintain your own in-house 'do not mail', 'do not telephone' and other channel-specific suppression lists to use alongside preference service files such as TPS, MPS, CTPS, BMPS, FPS and *Your Choice*.
- **Screen all communications against lists before use**
  Screen your contact lists against your relevant in–house suppression files as well as the appropriate preference service file before sending out any marketing communication.

Single customer view

- **Create 'single customer view' database**
  Compile all data about your customer into one file – a 'single customer view' – as a critical foundation for customer relationship management.

Screening and suppression

Your data will naturally start to decay as soon as it is collected, as your customers' circumstances inevitably change.

People move, get married, have children, change jobs, change their names – so if you do not screen for these changes your valuable customer and prospect data will quickly go out of date.

A few example statistics to represent the rate of data decay:

- In 2012-13, 2.3 million households had moved into their current accommodation in the previous 12 months. (Source: www.gov.uk – English Housing Survey Headline Report 2012-13)
- There were 499,331 deaths registered in England and Wales in 2012. (Source: Office of National Statistics)
- There are over 5.9 million records on the MPS suppression file – with around 19,000 new records added each month
- 102,000 new businesses were registered in 2012. (Source: Department for Business Innovation and Skills)
- There were more than 4500 UK business name changes per month in 2013. (Source: Companies House – Statistical tables on companies' registration activities 2012-13)
- In the UK, more than 20 million mailed items are incorrectly addressed every month, costing businesses an estimated £200m to £300m per year. (Source: DMA/Axiom whitepaper Reaching more consumers with certainty, 2011)

Why screen and suppress?

It is crucial to the success of your one-to-one marketing to screen your lists for gone-aways, deceased people and opted-out consumers – allowing you to only use accurate, effective data.

- **Improve your ROI**
  Use suppression and data screening effectively to improve your return on investment by filtering out the incorrect records that will waste your money and resources.
- **Maintain data to remain competitive**
  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.
- **Screen data regularly to preserve its integrity**
  Data decay cannot be avoided – so you must check your records against suppression and screening files regularly to ensure that your data remains accurate, up to date and effective in your one-to-one marketing.
- **Minimise reputational damage**
  Marketing to gone-aways and deceased people will only serve to damage your brand reputation, along with the reputation of our industry.
- **Enable effective campaign management**
  Suppression files play an important role in the effective management of CRM and one-to-one marketing.
- **Be compliant**
  It is a legal requirement and your obligation under DPA, the DMA Code and the CAP Code to screen your marketing lists against the relevant preference services before using them for one-to-one marketing purposes.
- **Be environmentally responsible**

Sending advertising mail to consumers who are never going to respond wastes an enormous amount of energy and materials.

Support our industry's efforts to do as much as possible to minimise wastage and improve the environmental performance of the industry.

Goals

- **Save costs**
  Cut out the direct and indirect costs associated with marketing to consumers who cannot or will not respond.
- **Improve list quality**
  Most customers and businesses either forget or do not bother to notify changes in their circumstances to organisations that hold their details on file.

  Use suppression files to improve the quality of the records you use for marketing purposes.
- **Improve data quality and richness**
  Enhance the data you held on customer files with updated information and preferences.
- **Regain contact with customers**
  Identify gone-aways as a first step towards maintaining or re-establishing contact with your customers.
- **Increase efficiency**
  Improve the efficiency of your marketing and telemarketing.
- **Improve targeting**
  Identify significant changes at either individual or address level, which you can use for targeting purposes.
- **Improve credit checking**
  Use for credit checking.
- **Identify legacy income**
  If you are a charity, use to identify legacy income.

Strategy

- **Target only relevant customers**
  The ambition of your one-to-one marketing activity must be to reach only those customers who are able and willing to respond.

  Suppressing invalid records will advance this goal and make your campaigns more effective, efficient and profitable now and in the future.
- **Grab the benefits**
  Do as much as possible, as promptly as possible, to make sure you enjoy the competitive advantage of using superior-quality data.
- **Identify poor prospects**
  Suppression files can indicate customers or businesses that have opted-out, moved address, changed status or details, no longer exist or are unlikely to be creditworthy.

- **Maintain internal suppression files**
  Maintain an internal suppression files of customers and prospects who have asked your organisation not to contact them – either in any form or via specific channels, such as email or telephone.

  You must match your campaign data against these files before despatch.

  Any matches identified must be removed from your campaign.

Suppression files

At a very simple level, these files contain the records of consumers who cannot or do not wish to respond to one-to-one marketing communications.

- **Suppressed records can include:**
  - Gone-aways – customers who have moved address
  - Deceased people
  - Opt-outs
  - Credit risks
- **Information contained in business suppression files can include:**
  - Businesses that have moved address
  - Customers whose employer has changed
  - Customers 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'
  - Businesses addresses that may be considered to be not the right address for marketing

DMA preference services

The DMA administers the preference services to allow consumers to stop unsolicited one-to-one sales and marketing communications.

It is your legal obligation to match your contact lists against these DMA preference service suppression files before sending unsolicited marketing communications:

Business-to-consumer

- **Telephone Preference Service (TPS)**
- **Fax Preference Service (FPS)**
- **Mailing Preference Service (MPS)**
- **Baby Mailing Preference Service (BMPS)**

Business-to-business

- **Corporate Telephone Preference Service (CTPS)**
- **Telephone Preference Service (TPS)**
  TPS registration covers the consumer as both a private individual and as a sole tader – so you must screen against TPS when conducting business-to-business calls as well as business-to-consumer ones.

Telephone Preference Service (TPS)

About TPS

- **Consumer telemarketing opt-out**
  The TPS is a list of consumers who have registered their telephone numbers in order to stop receiving unsolicited live telephone marketing calls.

  www.tpsonline.org.uk
- **Legislation governing TPS**
  The current legislation governing the TPS is PECR.
- **Permanent registration**
  Registration remains in place until a consumer changes their telephone number.
- **List size**
  The TPS file contains approximately 19.8 million records (May 2014) and is growing at a significant rate.
- **Obtaining the TPS file**
  TPS files are available to data processors or end users through payment of licence/subscription fees.

Your obligations under TPS

- **Comply with PECR**
  If you make unsolicited marketing telephone calls to customers, you must comply with PECR.

  This also applies if you work for a charity, voluntary organisation, political party or any business.
- **Do not call TPS registrants**
  It unlawful to make a call to a consumer who has indicated that they do not wish to receive such calls – whether they have registered with TPS or notified your organisation directly.
- **Clean all lists against TPS**
  Clean both 'cold' lists and customer lists against TPS before you make calls, to ensure regulatory compliance.
- **Comply within 28 days**
  You must comply with a request for the suppression of a telephone number no later than 28 days after it is registered with TPS.
- **TPS updated daily**
  The TPS file is updated daily.
- **Non-marketing calls not covered**
  TPS registration does not preclude calls from market research organisations, customer service calls and debt collection calls that fall outside the scope of the legislation.

Calling your own customers who are registered on TPS

- **You can call your own customers**
  You CAN call your own customers, even if they are on TPS, as long as you meet the following conditions:

  1. You have collected the telephone number directly from your consumer and not from the BT Osis or another file

     AND

  2. You told your customer that their telephone number will be used for one-to-one marketing calls

     AND

  3. You provided your customer with a clear opportunity, at point of colection, to opt-out from receiving such calls

- **You cannot call bought numbers on TPS**
  A bought or rented record does not count as your customer. If you have bought or rented a customer phone number and it is registered on the TPS, you cannot call it.

- **Question value of calling a TPS-registered customer**
  You should carefully consider whether to telemarket to a customer who is registered on TPS – even if you are legally able to.

  It seems fair to assume that a customer who is sufficiently motivated to register on TPS is not likely to respond positively to a telemarketing call from you.

- **Contact via other channels**
  Consider using a different communication channel to contact your customer.

Breaches

- **Enforced by ICO**
  If a breach of the regulations occurs it is the responsibility of the Information Commissioner's Office (ICO) to enforce the regulations.

- **TPS investigation**
  The TPS itself will investigate initial complaints made to it about an unsolicited marketing call made to a number registered on the TPS, but the ICO will determine what action it will take for breach of the Regulations.

- **Referral to Ofcom**
  The TPS may also refer an organisation to Ofcom if it is alleged to be in breach of regulation.

TPS Assured

- **Accreditation of TPS compliance**
  TPS Assured is an annual audit and certification service that assesses whether your organisation complies with PECR, Ofcom guidance and TPS Assured's guidance on outbound telemarketing best practice.

  If you are a UK-based organisation that uses outbound telemarketing to contact UK consumers, you can apply for TPS Assured certification.

- **TPS Assured helps your business**
  Achieving TPS Assured accreditation helps your business with three key benefits:

  - **Stay on the right side of the law**
    TPS Assured brings all the rules governing telemarketing together in one place to make it easier for you to comply and follow best practice.

    You will also receive expert advice, guidance and immediate updates about any changes to the laws, rules or regulations that could affect the telemarketing industry.

- **Gain competitive advantage**
  Use the TPS Assured logo on your website and corporate literature to differentiate your business from those who have not achieved accreditation.

  Accreditation also gives consumers confidence that you have been independently assessed.

- **Protect your reputation**
  Avoid the bad publicity and reputational damage of unwittingly breaking the law – as well as the hefty fines that come with it.

  The ICO and Ofcom have issued non-compliant telemarketers with millions of pounds of fines over recent years – and will crack down heavily on any rogue practitioners.

- **Find out more and apply for accreditation**
  For more information and to apply for TPS Assured accreditation, visit:

  tpsassured.co.uk

Corporate Telephone Preference Service (CTPS)

- **Corporate telemarketing opt-out**
  The CTPS is run in the same way as the TPS, but allows corporates to opt-out of receiving telemarketing calls to specific numbers.

  'Corporates' include 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.

  www.tpsonline.org.uk

- **Renewed annually**
  The registration has to be in writing and renewed every year.

- **Confirmed in writing**
  The CTPS will also send out a confirmatory notice in writing of registration.

- **Screen against CTPS and TPS**
  If you are carrying out B2B marketing then you need to screen against both the TPS file in respect of sole traders and partnerships and against the CTPS for limited and publicly limited companies.

Mailing Preference Service (MPS)

- **Administered by the DMA**
  The MPS is administered by the DMA on a not-for-profit basis.

  To find out more, find a list cleaning company or purchase the MPS suppression file, visit:

  www.mpsonline.org.uk/mpsr

- **Advertising mail opt-out**
  The MPS Consumer File is a list of names and addresses of consumers who have expressed a wish to opt-out of receiving unsolicited advertising mail.

- **Removes consumers from 'cold' mailing lists**
  The MPS is primarily used for suppressing consumers from 'cold' unsolicited mailing lists.

- **Records remain on MPS indefinitely**
  Names remain on the file indefinitely or until the MPS is notified by the consumer to remove them.

- **Updated monthly**
  The file is updated on a monthly basis.
- **Over 5.4 million suppressed records**
  The file size (as of October 2012) is in excess of 5.4 million records – with approximately 30,000 new records added each month.
- **Some data processors screen against MPS without charge**
  The MPS consumer file is held by most data processors and some may provide suppression matches to their clients without charge.
- **Level of suppression**
  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.
- **Funding**
  MPS is funded through a levy on Royal Mail's Mailsort service and a fee collected from licensees who purchase the data file.
- **MPS screening compliance**
  There is no legal requirement to use MPS against your existing in-house customer files, provided that:

  1. You offered your customers the opportunity to opt-out from unsolicited advertising mail at the point of sign-up

     AND

  2. You screen your mailing list against your own in-house do-not-mail list before each mailing

  However, in the opinion of the DMA and other industry bodies, screening against the MPS is now a legal requirement under *The Consumer Protection from Unfair Trading Regulations 2008*.

  It is important to seek your own legal advice on this specific issue.
- **DMA Code and CAP Code requirement**
  You must screen against the MPS Consumer File as a condition of the DMA Code and the CAP Code.

Baby Mailing Preference Service (BMPS)

- **Mail opt-out for bereaved parents**
  The BMPS entitles parents who have suffered a miscarriage or bereavement of a baby in the first weeks of life to register their wish not to receive baby-related mailings.

  www.mpsonline.org.uk/bmpsr

Facsimile Preference Service (FPS)

- **Fax opt-out**
  The FPS is a register of individuals and businesses that object to receiving unsolicited marketing faxes.

  www.fpsonline.org.uk
- **FPS governed by PECR**
  The current legislation governing the FPS is PECR.
- **Do not fax FPS registrants**
  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).

- **FPS covers cold AND customer lists**
  The scope of the legislation covers faxes made to both 'cold' lists AND customer lists.
- **Comply within 28 days**
  You must comply with a request for the suppression of a fax number no later than 28 days after it is registered with the FPS.
- **Updated daily**
  The FPS file is updated daily.

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.

- **Access files through data supplier**
  Specialist companies use a range of different methods and sources for compiling suppression files, which are then made available to you mainly through the data processors that license the data.
- **License files directly for high volume**
  Some high volume data users choose to have direct licensing arrangements with the file owner.
- **Research suppression products**
  Most data processors have a suite of different suppression products available.

  Some of these files offer similar data but use different sources and methods to compile the data.
- **Be aware of different suppression matching results**
  The processes used by data processors 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.

  The differences in processes used to 'match' records on suppression files account for most of the variations in results amongst data processors' matching on identical data sets.
- **Take data processor's advice**
  As part of any standard data hygiene or campaign preparation process, ask your data processor to advise you of any records on their lists that match records on these suppression files.
- **Define suppression processing with data processor**
  Once a suppression match has been identified, you can make an informed choice about the way in which the record is processed – for example, which records should be suppressed and which should not.

Choosing your data screening and suppression products

The perfect screening product would identify all changes immediately and 100% accurately.

Whilst in reality this is never likely to happen, you can assess your screening and suppression products based on how close they get to this ideal.

The key criteria to look for in a product are market coverage, accuracy and recency.

Market coverage

- **Assess product against your needs**

Assess the market coverage offered by each product against your business needs.

For example, if you are looking to conduct a nationwide mailing campaign then, with 1.5 million UK households moving each year, a product collating just 0.65 million consumer records annually will only ever be able to provide a part of your gone-away suppression solution.

Accuracy

- **Understand verified vs assumed data changes**
  Data for suppression files is obtained from many sources.

  Some of these sources are verified, with the change in circumstance known to have happened – for example, using a death registration number.

  Other changes are assumed – for example, flagging a gone-away based on a certain amount of returned mail.

- **Scrutinise to preserve data integrity**
  Inaccuracy in suppression files will lead to over-suppression and remove records from your database or prospect file that have not changed.

- **Test accuracy regularly**
  It is therefore important to test suppression files for accuracy as well as match rates.

- **Treat different data lists appropriately**
  Suppress data appropriately according to its value.

  For example, it might be wise to treat customer and prospect data differently to reflect the different value of each relationship.

- **Be wary when confirming gone-aways**
  Postal returns sometimes do not indicate a gone-away, but rather a disgruntled customer or prospect.

  To illustrate – in 2005, the average do-not-mail file had around 42% of supposed gone-aways still living at the address, with mail sent back by consumers as a way of trying to get their name taken off a database.

Recency

- **Keep data constantly up to date**
  The longer it takes for you to know that your customer has moved or even died, the more damage you will do to your brand and the less efficient your marketing will be.

- **Fit screening schedule to business needs**
  Screen as often as you run campaigns.

  For example, if you send on a monthly basis you need a suppression solution that keeps your data accurate at this pace; similarly, if you only run campaigns annually then you might only need to screen and suppress once a year.

- **Typical screening frequency**
  Most gone-away solutions are now monthly – and 'deceased' solutions are getting faster, with one supplier now providing daily updates.

Responsibilities

Client responsibilities:

- **Provide clear brief**
  Provide a clear written brief – including a hierarchy of suppression files to be used.
- **Provide further information**
  Provide any further information requested by your supplier in a timely fashion.
- **Check files are appropriate**
  Ensure with your supplier that correct files are being used to suit your data and your marketing requirements.
- **Sign off promptly**
  Where you have requested a data audit (i.e. a sample of the file with verification of matching), check and sign it off promptly.

  Look closely at your suppression match results and surrounding issues to ensure a satisfactory level of accuracy.
- **Understand your accountability**
  As the data controller, it is your responsibility to make sure that the data you use is fully compliant – the buck stops with you.

  Ensure that you have necessary procedures, resources and policies in place to reliably manage this responsibility.

Supplier responsibilities:

- **Check brief**
  Check that your client's brief is clear and that you have understood it correctly – with any special processing requirements clarified and agreed.
- **Advise on data strategy**
  Advise your client how to get the best results for their data and their marketing requirements.
- **Ensure best practice**
  Ensure your client is aware of best practice.
- **Communicate promptly**
  Advise your client as soon as possible if there are any problems with the data you have been asked to process.
- **Stick to hierarchies**
  Use suppression hierarchies according to the brief – with sample matches supplied if required.
- **Provide reporting**
  Provide audit reports to show the progress of records through your process – including how many records have been suppressed and why.

  Raise any queries with your client as soon as possible.

Subcontracting data hygiene

Selecting your data processor

The range of services, methods and capability for data capture and processing services varies widely between processors.

It is vital to choose the right organisation that can most appropriately cater for your needs, rather than purely placing your data with the cheapest processor, to give you the highest-value data as well as confident compliance.

Understand the two stages to data capture for which you should assess prospective data processors:

1. **Data entry**
    - Convert written, printed or telephone responses into a digital data file via optical scanning, re-keying or transcription
    - Produce a list that is identical to the responses received, with information exactly as collected
2. **Data processing**
    - Validating, correcting and enhancing this data

Key criteria for selecting a data processor

- **Nature of your requirements**
  Clearly understand your data processing needs, including the level of accuracy required and the extent of further work needed on a file, before attempting to choose your data processor.
- **Relevant experience and expertise**
  Data capture may be carried out from market research surveys, postal lifestyle questionnaires, coupon responses, and so on. Each of these employs a different skillset and possibly different technologies to handle.

  Make sure you conduct due diligence to engage a supplier with the appropriate knowledge.
- **Range of data facilities**
  Select a data processor that can offer the necessary facilities if you might need to validate or enhance your data.

  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.
- **Secure electronic transfer**
  If frequent, regular data transfers are required, always use a data processor with secure electronic transfer facilities.
- **Environmental compliance**
  Choose a supplier that has a strong environmental policy and a commitment to improvement.

  Your data processor should offer the following services, which are necessary to produce data that maximises efficiency and minimises material wastage – thus facilitating high environmental performance in your marketing activity:
    - The capability to suitably manage and match customer suppression files against mailing cells
    - The capability to make selection and extractions from data
    - De-duplication of data to varying levels – at least to individual, family, household and business site
    - Address verification, enhancement and summary report generation with the Royal Mail Postcode Address File (PAF®)
    - Suppression of prospect data against the Mailing Preference Service (MPS)
    - Suppression or enhancement against commercially available deceased and gone-away files

Engaging an offshore data processor

- **Ensure compliance of offshore data processor**
  Many suppliers of data capture are based offshore and can offer you significant savings, even when allowing for freight costs.

  But be aware of the eighth principle of the DPA, which governs the transfer of data outside the European Economic Area (EEA).

  To comply with the law, data is only allowed to be exported outside of the EEA:

  - To countries that have an adequate level of data protection

    OR
  - Where contractual arrangements are put in place between the organisations involved to ensure an adequate level of data protection

- **US and Europe – Safe Harbor Agreement**
  A Safe Harbor Agreement currently operates between the US and Europe.

  The Safe Harbor Agreement is a self-verified, self-certified, voluntary scheme under which US firms pledge to protect data from European partners in accordance with European law.

  A list of US firms subscribed to the Safe Harbor Agreement can be found at:

  http://export.gov/safeharbor/

- **Check outsource country status**
  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

- **Seek legal advice before transferring**
  You are strongly advised to consult the DMA's legal department or your own legal advisers before transferring data out of the EEA.

Getting started with your data processor

- **Agree brief**
  Agree the format and schedule for data output in advance.

- **Obtain written agreements**
  Obtain signed, written agreements in advance of any work being undertaken.

- **Cover liability**
  In addition to standard contractual obligations, make sure these also cover liability for data and confidentiality.

- **Agree data transfer**
  Agree whether responses will be sent for data capture and returned in batches, or as a single consolidated set.

- **Agree file formats**
  Documents may be converted into digital or optical files for faster retrieval and ease of storage.

- **Develop original documentation retrieval plans**
  Ensure that you have agreed plans for the retrieval of original documentation.

  This may be a legal requirement for some product categories, in case a dispute or query arises.

- **Agree documentation disposal plans**
  Ensure that correct procedures have been agreed for the disposal of all original documents, including incineration or shredding as appropriate.

Data care

Benchmarking

- **Agree accuracy rate for data capture**
  Agree the level of accuracy for data capture in advance with your data processor.
- **Define accuracy for each job undertaken**
  This is usually expressed in percentage terms – for example, '% rejects' and '% invalid addresses'.
- **Request test file**
  Request and check a test file to ensure these levels are being met – for example, you might choose to check a '1-in-N' sample or a random sample of the final file.
- **Agree accuracy rate for data matching**
  Agree a separate rate of accuracy for matching to address verification files, if data is to be validated and enhanced. Also specify the type of verification and definition of a match.

Responsibilities

Client responsibilities

- **Ensure accuracy is prioritised**
  Methods of data collection are designed to maximise accuracy, legibility/audibility and completeness of information supplied by customers.
- **Ensure supplier compliance**
  Suppliers comply with data protection laws, as appropriate.
- **Supply clear specifications and standards**
  Specifications for data capture are supplied, agreeing and stating levels of accuracy and matching required.
- **Ensure appropriate procedures are in place**
  Procedures are in place for retrieval or destruction of original documents after data capture.

Supplier responsibilities

- **Only accept appropriate work**
  Only accept work for which you have the appropriate skills and technology.
- **Keep tables up to date**
  Make sure your verification tables are maintained up to date.
- **Ensure compliance and security**
  Ensure that data and documents are processed, stored securely and, once you have completed the work, are returned or disposed of in line with the DPA and your client's brief.

Sharing data

Today it is very likely that you will need to share data with third parties for various essential business processes – such as for analytics software, email marketing, processing data for campaigns, CRM and administration of your own employee payroll.

The same rules apply for any business process that you outsource.

Your obligations are always the same around contracts, data transfer processes, and the responsibilities between controller and processor.

Seventh principle of the DPA

The seventh principle of the DPA applies to you even if your business uses a third party to process personal information on your behalf.

It 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."*

Third-party data processing contracts

In order to comply with the seventh principle of the DPA when outsourcing any data process to a supplier, you must:

- **Ensure security measures are in place**
  Choose a processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out.
- **Take responsibility for third-party compliance**
  Take all reasonable steps to ensure supplier compliance with those measures.
- **Have a written contract**
  All data processing must be carried out under contract which:
  1. Has been made or evidenced in writing

     AND
  2. Dictates that the supplier is to act only on instruction from the data controller

     AND
  3. Requires the supplier to comply with obligations imposed on their client by the seventh principle of the DPA
- **Data processing agreement**
  Use the suggested DMA data processing agreement and guidelines:

  dma.org.uk/article/data-processing-agreement-template
- **Use DataSeal**
  DataSeal is the industry standard for security of data handling and covers the transfer or data between two parties.

  DataSeal is administered by the DMA.

  For full information and to apply for accreditation, see the *DataSeal* section of this guide or visit:

  dma.org.uk/content/dataseal

Receipt and transfer of data

The transfer of data files is a basic, but critical process.

A project may involve the sourcing and transfer of hundreds of separate files, with a delivery schedule covering several weeks – so managing and controlling this process is critical to your orderly and compliant handling of data.

- **Always comply with the DPA**
  All transfers, handling and storage of data must comply with the DPA.
- **Check data security measures**
  You must ensure that all personal data is protected by appropriate security measures and processes when either receiving or transferring data.

  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 – and that only appropriate, authorised people can access the data.
- **Protect data subject's privacy**
  Always treat your customer's data as confidential.

  You must ensure at all times that your customer's privacy is protected and the obligations imposed by the DPA are followed as a minimum.
- **'Confidential' default status**
  If in doubt as to the classification of any data, err on the side of caution and use a 'confidential' default status.
- **Ensure data is backed up**
  Data should always be backed up and archived.
- **Ensure secure environment**
  All files must be stored and processed in a secure environment, appropriate to the sensitivity of the information.
- **Supply file layout**
  Supply documentation of each file layout to allow your data processor to prepare conversion procedures.
- **Supply data dictionary**
  Supply a data dictionary – this is a document to define what you expect to find in each data field.

  For example, you might define age categories, where A = 18-24, B = 25-34, C = 35-44, and so on.
- **Notify each file to your data processor and log each file on receipt.**
  Accurate management of files in this way will allow cross-checking of planned data use with actual use.
- **Confirm file details**
  On receipt, your data processor should confirm the file layout, size, readability, and status against your data schedule.
- **Notify file transfer format**
  Notify your data processor of the format in which each file will be delivered, along with any unusual media to be used.
- **Re-supply data if incorrect**
  Re-supply data if a file does not tally with the documentation, or if it is corrupted.

Data transfer process

The following guidelines are intended to offer a minimum requirement for the technological processes that you should follow when transferring data between two locations.

The aim is to ensure that all parties in the data transfer chain are following these minimum recommendations.

- **Scope of guidance**
  This guidance offers some basic best practice advice on technological measures to protect the security of data transfer – but does not address legal, compliance or any other procedural legislation.
- **Applicable to EEA**
  This guidance only covers recommendations for data transfer between countries within the EEA.
- **Transferring outside EEA**
  For data transfers to other countries please see the *Engaging an offshore data processor* section of this guide.

Before transfer:

- **Considerations**
  Before you transfer any data, consider:

    1. **Is the transfer really necessary?**
       Do not move data unless you really need to!
    2. **Are you transferring more than is needed?**
       Reduce the amount of data you move to reduce the risk and consequential damage if it does get lost.

       Consider sending only those records that are needed or only the specific fields that are required.
    3. **Are you certain that the recipient of your data is authorised to receive and process it?**
    4. **Are you certain that your recipient has adequate security measures to safeguard your data?**
    5. **Do all parties have the correct data protection notification?**
    6. **Are there sufficient security measures in place?**
       Including encryption, pseudonymisation and transfer methods.

Methods of transfer

Having ascertained that a transfer is required and reduced the data to the minimum necessary, it is important to consider HOW the data will be transferred.

Many methods of moving data from place to place are available – but the main ones to consider are as follows, listed in order of preference for guaranteeing the maximum level of security.

Secure File Transfer Protocol (SFTP)

- **About 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
    - With SFTP sending usernames and passwords in clear text is a thing of the past
    - 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

- **Encrypt files separately**
  Separately compress and encrypt files BEFORE transfer so that access to the data is still controlled once on the recipient's server.

  Various software applications are available for this – research to find the most appropriate for your purpose.

- **Set strong passwords**
  Passwords used for both file compression and the SFTP session should be unique and strong – meaning at least 10 characters, containing both numbers and letters and not based on a dictionary word.

- **Exchange passwords separately to the files**
  Ensure that passwords are exchanged securely – and separate to the data files.

- **Expire passwords**
  SFTP passwords should expire after a suitable time period.

- **Log all transfers**
  All transfers should be properly logged to enable proof of delivery – and to check that downloads are only actioned by authorised parties.

- **Remove files from SFTP servers immediately after transfer**
  Data should be promptly removed from your SFTP servers after download by the recipient and in accordance with your organisation's data retention policy.

File Transfer Protocol (FTP)

- **About 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
  - FTP is not as secure as SFTP but, if the additional guidelines below are followed, is probably better than the alternative methods listed

- **Encrypt files separately**
  Because FTP does not automatically encrypt data, you should compress and encrypt files using another software before transferring via FTP.

- **Be extra secure with passwords**
  It is even more important that the rules above relating to passwords and removal of data are followed.

- **Log all transfers**
  All transfers should be properly logged to enable proof of delivery – and to check that downloads are only actioned by authorised parties.

- **Remove all files from servers immediately after transfer**
  Data should be promptly removed from your FTP servers after download by the recipient and in accordance with your organisation's data retention policy.

FTP/S

- **About FTP/S**
    - This is the same protocol as SFTP but with data encrypted using Secure Sockets Layer (SSL) encryption
    - If you use this protocol, check that your server is configured to encrypt both the authentication and the data transfer layers – as often only the authentication is encrypted
    - If both encryptions are enabled then this method is at a similar level of security to SFTP and has the added advantage of not requiring anything other than a browser to access

HTTP/S

- **About HTTP/S**
    - This protocol is often used for files being downloaded from web servers
    - It can be very secure and is very convenient to the end user as files can be downloaded easily via web links and email links
    - It should be noted though that it is probably only suitable for relatively small files as transfers cannot be resumed if interrupted and have to be restarted from the beginning

Physical transfer by courier or post

Physical media transfer carries a much higher risk of data getting lost, damaged or delivered to the wrong person.

If this is the only method of data transfer available then the following guidelines should be followed:

- **Depersonalise**
  Ensure that your data is minimised – and preferably depersonalised.

  See the *Pseudonymising* section of this guide for further information.
- **Encrypt**
  Protect the data with strong encryption – AES256 is recommended.
- **Use strong passwords**
  Send strong, unique passwords to your recipient by a separate means.
- **Use specialist data couriers**
  Use a courier with a specialist data service if possible.
- **Have good contracts**
  Have a good contract with your courier service.

  If this is to be regular and the data is high value, consider asking to see your courier's security policies.
- **Confirm delivery**
  Confirm delivery with your recipient.
- **Check signatures**
  Ensure that signatures and receipts are readable and available quickly.

Email

Transferring data via email is not desirable and should be avoided if possible.

The main problem with email 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 both sender and recipient and on the email servers of the respective locations.

If this kind of transfer is unavoidable then the following guidelines should be undertaken:

- **Depersonalise**
  Ensure that the data is minimised and depersonalised.

  See the *Pseudonymising* section of this guide for further information.
- **Encrypt**
  Protect the data with strong encryption before attachment – AES256 is recommended.
- **Use strong passwords**
  Send strong, unique passwords to your recipient separately – preferably by telephone rather than another email message.
- **Check tracking receipt**
  Ask for a tracking receipt so you know when the email is opened.
- **Delete email from all email folders**
  Delete the attachments/sent email, plus and draft copies, after the message receipt is confirmed.

Responsibilities of data controller and data processor

Top tips

- **Define responsibilities**
  Ensure everyone in your organisation understands their responsibilities regarding the transfer and storage of data.
- **Classify data**
  Classify data so that everyone in the process can recognise its importance and sensitivity.
- **Send data securely**
  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 *Sharing data* section of this guide.
- **Use dummy addresses**
  We recommend the insertion of unique dummy addresses or 'seeds' into every data extract so that you can monitor all subsequent use and can quickly identify and stop any misuse.
- **Include all documentation**
  Ensure documentation is sent with all data, including file layouts and volumes.
- **Check delivery**
  Make sure you receive proof of delivery of your data.
- **Check received files**
  If you are receiving data files ensure you check them, in a timely manner, against your sender's documentation to validate the contents.
- **Store data securely**
  Store data in a secure environment, ensuring adequate backups and archiving takes place.

Data care

Client responsbilities

- **Supply schedule**
  Supply a schedule of all files to be used in advance.
- **Notify about media**
  Provide notification of media to be used, including uncommon formats.
- **Comply with DPA**
  Ensure all use of data complies with the DPA and is held, disclosed and processed lawfully – with a data processing agreement in place. See the *Data processing agreements* section for further information.
- **Provide file documentation**
  Provide full documentation for each file – covering project reference, file layout, supplier contact details, sample print, number of records and return instructions.
- **Supply test files**
  Supply test files when requested by your supplier.
- **Meet delivery schedules**
  Meet all delivery schedules as agreed.
- **Maintain data security**
  Ensure reasonable steps are taken to ensure that files are supplied free of viruses.
- **Check disaster recovery plan**
  Ensure that your supplier has a proven and robust disaster recovery plan in place – sufficient to protect your data and your project. Give consideration to the nature and value of your project being undertaken.

Supplier responsibilities:

- **Check files against schedule**
  Check all files that you receive against your client's schedule.
- **Check file condition**
  Check all files for readability and size.
- **Raise any issues**
  Promptly notify your client with any discrepancies or problems.
- **Comply with DPA**
  Process and store all data in compliance with the DPA. See the *Data security and storage section* of this guide for further information.
- **Check files for corruption**
  Check all incoming data for viruses and inform the data owner immediately of any problems.
- **Follow schedule**
  Follow the agreed data processing schedule – and notify your client immediately about any changes or delays.
- **Give files unique IDs**
  Give each file a unique code so it can be reconstituted at the end of the project and tracked through processing.
- **Return data in agreed format**
  Return data to your client in the agreed format upon completion of your project.
- **Have appropriate insurance**
  Make sure that your organisation has the appropriate professional indemnity insurance to cover your liability for loss, damage or theft of data whilst in your possession or during processing.

Data security and storage

Be diligent with data

Consumer trust is one of the most valuable attributes your organisation can possess.

In this time of identity theft and fraudulent activity it is critical that your organisation takes every precaution when handling personal data.

Inadequate care or inappropriate handling of data can have a significant impact on customer perception of your brand – with obvious implications for customer retention, as well as wider legal implications for your organisation.

Strategy

- **Assess risks**
  Assess security risks throughout your business and processes.
- **Engage senior staff**
  Make sure your senior management are aware of and engaged with the importance of data security.
- **Have policies and practices in place**
  Whatever your organisation, make sure you have policies and practices in place to ensure that your consumer data is correctly collected, maintained and protected.
- **Define systems**
  Have a well-defined system in place to ensure your data is kept secure at all times.

  Include a robust risk assessment and clear definition of who has access and which employees have roles and responsibilities in specific areas.
- **Audit regularly**
  Your policies and practices should not exist in isolation and should be subject to audit, review and updating on an ongoing basis.
- **Define remediation**
  Ensure you have policies and practices that govern what should happen if a data security breach has occurred (including at a third party).

  This should include how you notify affected customers and potentially the wider public – as well as how your organisation should handle any enquiries, press coverage, brand damage or other consequences.

Security measures

You must take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data – and against accidental loss or destruction of, or damage to, personal data.

For example, your business procedures should ensure that you:

- **Store and dispose of data securely**
  Ensure no customer or prospect data is left lying around or discarded in waste bins where it could ultimately end up in the wrong hands or in the public domain.
- **Handle data in a controlled environment**
  Make sure that computer screens displaying personal data are not visible to unauthorised personnel.

- **Verify customer identities**
  When handling enquiries by phone, which might result in personal data being discussed or revealed, ensure that the identity of your customer is verified at the beginning of the call.
- **Control access to data**
  Limit access to customer data to only those staff who need access to perform their official duties.
- **Define staff responsibilities**
  Inform your staff that unauthorised use or disclosure of customer data is a serious disciplinary matter.
- **Check third-party access**
  If your customer's information is stored externally or accessed by third parties, you have an obligation to understand what policies and practices the third party has in place and make sure they match up to your own.
- **Further information**
  For full information see the DMA *Best practice in information security*:

  dma.org.uk/sites/default/files/tookit_files/Best-practice-information-security.pdf

DataSeal

- **Use DataSeal to demonstrate compliance**
  DataSeal is an accessible, achievable and cost-effective way to show you have the right information security measures in place.

  DataSeal is the only recognised standard for information security management systems other than ISO 27001.

  This private standard is available to both client and supplier organisations who are DMA members or members of any participating trade association – such as the IPA, IPM or ISBA.
- **DataSeal criteria**
  DataSeal sets out performance requirements for:
    - Risk assessment
    - Management responsibility
    - Traceability and responsibility of data
    - Acceptable use
    - Access control
    - Passwords
    - Virus and spy prevention
    - Internet and network security
    - System and server security
    - Back-ups
    - Data storage and elimination
    - Outsourcing
- **Audit your data security**
  The DataSeal self-assessment questionnaire is a useful way to assess your data security measures and identify areas that need improvement.

  Take the questionnaire at:

  dma.org.uk/content/self-assessment-tool

- **Sign up for DataSeal**
  For full criteria, and to apply for accreditation, visit:

  dma.org.uk/content/dataseal

Training staff to handle data

- **Train data-handling staff**
  Train all staff to understand the importance and best practice for data security and handling.
- **Clarify roles**
  Make all staff properly aware of their individual responsibilities for information security.
- **Keep staff knowledge up to date**
  Keep staff knowledge up to date as legislation, industry standards and consumer attitudes evolve.

Data handling environments

- **Consider security measures against sensitivity of data**
  Weigh up the value and sensitivity of the data your staff have access to and create an appropriate work environment.

  At the top end, organisations that handle extremely sensitive financial or other personal information already create high-security environments in which staff are not allowed pens, paper, phones or any other means or copying or removing data.

  As data regulations continue to tighten and the consequences of a security breach increase, it is wise to err on the side of caution to protect both your organisation and your data-handling staff from the chance of a breach.

Acceptable use

- **Define 'acceptable use policy'**
  Ensure staff understand and comply with your 'acceptable use policy' for all data handling.
- **Define disciplinary policy**
  Have a formal disciplinary policy in the case of information security breaches – and make sure your staff know, understand and have agreed to this.

Access control

- **Identify individual data handlers**
  Use unique and individual authenticated logins for each member of staff.
- **Restrict network access**
  Ensure access to your network is restricted only to appropriate, fully-trained and accountable personnel.
- **Restrict physical access**
  Restrict physical access to your data systems similarly.
- **Control visitor access**
  Make sure visitor access is appropriately controlled and safeguarded.
- **Check third-party policies**
  Ensure that any third parties who have access to your data also have sufficient security measures in place.
- **Review access rights regularly**
  Put in place a formal process for reviewing and removing access rights of staff movers and leavers.

Data care

System security

- **Test your security systems to breaking point**
  Test your security systems as robustly as possible – you should hope to discover any possible weakness during testing rather than when a breach happens for real.
- **Assess and test security of third-party tools**
  Almost any business now handles their data through third-party tools – for example, a payroll system, an email marketing platform or a website content management system.

  No matter how robust your internal data security is, you must interrogate the security of any third-party systems you use as these are likely focal points for careless data handling and malicious attack.
- **Keep system up to date**
  Update your systems regularly with the latest antivirus updates, patches and general security updates.
- **Maintain servers regularly**
  Regularly or automatically run server maintenance and review logs.

Network security

- **Use robust firewalls**
  Make sure all connections to the internet and to any external parties go through robust firewalls
- **Use latest encryption standards**
  Secure your wireless networks with the latest encryption standard – such as WPA2.
- **Review standards regularly**
  Regularly or automatically review these standards – as, like WEP encryption, they can become out of date and vulnerable as technology advances.

Viruses and spyware

- **Use robust antivirus software**
  Use a recognised antivirus solution on all servers, desktops, workstations and entry and exit points to your data systems.
- **Define disciplinary policy**
  Have a disciplinary policy in place for personnel who deliberately or acidentally introduce a virus – and make sure your staff are fully aware of this policy.

Passwords

- **Use secure passwords**
  Make sure all passwords:
    - Are at least 10 characters long
    - Use a combination of alpha and numerical characters
    - Do not use dictionary words
    - Are changed regularly

Data care

Back-up

- **Back-up data securely**
  Have a thorough, frequent and up-to-date back-up process.
- **Use off-site back-up**
  Have on-site and off-site back-up storage.
- **Test back-ups regularly**
  Test back-up systems regularly.

Traceability

- **Log data transfer**
  Log all client data on receipt and despatch.
- **Encrypt data during transfer**
  Encrypt data during transfer, transmission or delivery to third parties or external systems.

Data elimination

- **Define data disposal policy**
  Have robust, documented processes in place to handle data storage and elimination.
- **Keep records**
  Keep data disposal records/logs.

Data usage

Privacy Impact Assessments

Privacy Impact Assessments (PIA) are a successful tool to help you identify your data requirements, security, issues and strategy on a campaign-by-campaign basis, and are an important safeguard of customer privacy rights.

In essence, a PIA is an audit of the implications of your proposed data usage and collection for your customer – and will help you to prevent any nasty surprises and unforseen consequences during your project.

PIAs are a virtuous cycle – covering your organisation from a compliance perspective, enabling you to ask the right questions of data providers, tightening up your campaign goals and making you and your organisation better at marketing.

Goals

- **Interrogate and streamline campaign data requirements**
  Complete a thorough PIA as an exercise to force your campaign team to detail and justify your data requirements.

  This is a highly valuable exercise that will help you to filter out unnecessary data collection or usage that might otherwise waste time and resources to administer – or even potentially put you in contravention of the DPA.

- **Strategise data collection**
  Use your PIA to define your data collection strategy – including what data you wish to collect and why, as well as how you can capture it with maximum conversion.

- **Improve project goals and success**
  A good PIA will help you refine your project goals and therefore be more efficient and successful in realising them.

- **Integrate with project management**
  Make your PIA a central part of your project management.

  Data lies at the heart of any campaign, so it is both useful and logical to use your PIA to co-ordinate the efforts of different teams working across different media.

- **Identify problems**
  Your PIA will help you to identify any issues surrounding your data, or related campaign delivery issues, at the planning and testing stage – making them much easier and less costly to fix than if you stumble across them after campaign launch.

- **Protect brand reputation**
  Identifying potential risks before launching your campaign will safeguard your brand against potentially significant reputational damage, as well as the possiblity of official sanctions or penalties.

- **Be accountable and auditable**
  Keep a record of your PIA for each campaign in case of future audit or dispute.

  The ICO initiated PIAs and may appreciate the existence of a PIA as proof of your good intentions when investigating any complaint or dispute.

Strategy

- **Conduct a PIA before each campaign**
  Carry out a PIA before each campaign to help your team optimise its data goals, campaign goals, strategy, plans and processes.

- **Conduct a PIA to review or change existing systems**
  Carry out a PIA to interrogate any existing or new project – for example, as part of your planning process when selecting and implementing any new system through which customer data will be handled.

- **Ask the difficult questions**
  It might even be that a thorough PIA reveals too many holes in your project strategy or viability and that you abandon the project entirely, as a result.

  You should still see this as a good thing – potentially saving you wasted time, resource and reputational damage.

- **Learn trends**
  By conducting PIAs before every project, you can quickly begin to spot patterns that could lead you to identify underlying system improvements, to spot new data opportunities or to implement major efficiencies.

  Use PIAs as an inexpensive opportunity for continual improvement for yourself and your team.

- **Further guidance and templates from the ICO**
  PIAs were initiated by the ICO and their website offers thorough guidance on how to create and fully benefit from your PIA – as well as offering examples and templates.

  Find out more at:

  ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

Using webforms, social APIs and plug-ins

- **Assess security**
  Forms and plug-ins are potential data security weakspots – so take thorough measures when using third-party webforms that they are secure and cannot be viewed or hacked.

- **Data access and ownership**
  Understand the terms and conditions of any third-party sites you link to.

  For example, if your customer merely shares content from your site via Facebook, then Facebook will now know that your customer has been on your site – information that could be deeply personal if, for example, your site covers religious, ethnic, political, sexual, trade union or any other sensitive content.

  Work through your customer's journey thoroughly to ensure that their privacy is not compromised in any way, whether actually or potentially.

Anonymisation and pseudonymisation

Anonymisation is the practise of stripping out your customer's personally identifiable information (PII) from your data in order to be able to easily transfer, process and segment it.

Pseudonymisation differs from anonymisation in that whilst your customer's PII is stripped out, a code is typically assigned instead – for example, "Joe Bloggs" becomes "Customer 12345". This means that processing work done to the data can be re-applied to your customer's personal records later on to facilitate more relevant and effective one-to-one marketing.

The key difference you should be aware of is that completely, irreversibly anonymised data is no longer subject to EU data protection regulation – but pseudonymised data, since it can be re-identified later by means of the code attached to it, is still absolutely subject to all the regulations and best practice of the DPA, PECR and industry codes.

- **Consumer PII includes:**
    - Name
    - Address
    - Phone numbers
    - Email addresses
    - Credit card details
    - Bank details
    - Organisation account or membership numbers
    - National Insurance number
    - Driver's licence
    - NHS medical number
    - Date of birth

Goals

Anonymisation and pseudonymisation make it possible for you to process your data more easily, such as being able to:

- Handle data outside of data protection restrictions
- Pass data over to analysts to create segments or conduct analysis
- Process and transfer your data more securely
- Not need to tell customers about data breaches – because no individuals will be personally identifible from the misplaced data

Pseudonymisation

- **Use ONS output areas, not postcodes**
  Use Office for National Statistics (ONS) output areas as your lowest level of geography for identifying data, rather than postcodes.

  Postcodes are specific enough that they could be combined with other data, such as age or ethnicity, to identify an individual customer – whereas ONS output areas are typically a group of five or more postcodes.

- **Use random code to map data processing back onto consumer record**
  You can leave a randomly-generated key within each record.

  This enables you to send pseudonymised data to a third party for data processing work – such as segmentation – but then be able to match this processing work back onto the original file afterwards.

Further information

For more detailed guidance on anonymisation, see the ICO's *Anonymisation: managing data protection risk code of practice*:

ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

Data tagging and enhancement

You can tag records with additional information – such as adding your customer's personal preferences to their name and address record.

Aims

There are many ways that both your business and your customer can benefit from enhancing your data, including:

- **Targeting**
  Be able to target more relevant messaging to each individual customer.
- **Dynamic content**
  Be able to target variable content to different customer segments in response to their behaviour.
- **Personalisation**
  Be able to personalise your message to your individual customer – whether online or offline.
- **Efficiency**
  Better efficiency and environmental performance of your campaign.
- **Business insight**
  Be able to see your customer lifecycle more clearly and use this to identify improvements.

Approach

- **Set goals**
  Be clear about why you are enhancing your file with external data.
- **Identify best enhancement fields**
  If you are buying external data for use in targeting models, test which variables will give you uplift before buying.
- **Benchmark value of enhancement**
  Use a control cell to determine the additional value the enhanced data is supplying.
- **Retest variables regularly**
  Retest data variables every year as the profile of your customers may change.

Data usage

Data appending

- **Enhance your customer records to improve marketing**
  Append further information to your customer records to enable you to send more targeted, relevant and rewarding communications.
- **Collect data directly from customer**
  It is always better to collect further information directly from your customer – and to tell them why you need it and how it will benefit them.

  If you are not confident you can justify it to your customer, re-evaluate the value of appending and using this data – and consider the likely response you will get from your customer.
- **Have a clear business or customer benefit**
  If you do enhance data, make sure it will either add a customer or business benefit in terms of more accurate targeting (when adding profiling) or more relevant, effective communication.
- **Only append to customer data**
  Do not append to prospect data or inactive, lost customer or old data.
- **Check opt-in**
  Ensure that ALL of the data that you are appending is opted-in.
- **Gather customer preferences**
  In each communication you send, offer an easy way for your customer to define their communication preferences or to opt-out completely.
- **Understand channel-specific rules**
  There are specific data appending rules for different channels – particularly for email and mobile devices.

  Refer to the specific guide for further information or members can contact the DMA legal team for advice.

Using bought data for enhancement

- **Check recency of bought data**
  Check how up to date the data you are buying is – including when and how was it collected.
- **Check accuracy of bought data against known data**
  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.
- **Set matching levels**
  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 customers living in the same household.
- **Be careful using modelled data**
  Do not 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.

Targeting and segmentation

Profiling

- **Identify common traits within your customer base**
  Carry out profiling on your data to identify particular traits that make a customer more likely to buy from you.

  For example, you might discover that a particular age range, geographic area or income range of customers responds more positively to your marketing.

- **Use profiling to increase returns**
  Naturally, profiling gives you better-targeted data with which to deliver more effective, efficient, relevant and profitable campaigns – as well as improving brand reputation and awareness.

  Measure your campaign and financial returns against your investment to ensure that your profiling is productive.

- **Match data to highlight prime consumers**
  Match your customer files against external resources to identify the best prospects for each particular offer, product or service.

- **Fit profiling process to campaign goals**
  This process can differ considerably depending on whether you are looking to communicate with consumers who have not yet purchased from you – or those with whom you have an existing relationship.

Segmentation

- **Define different customer groups**
  Use data variables identified through profiling to define different customer groups within your lists.

  There are many ways to divide a list of customers – you might choose to segment by age, location, income, buying history, lifestyle choices or communication preferences.

- **Segment to increase response or conversion**
  Define your campaign selections to give an increased likelihood of response or conversion when compared to a random selection.

- **Use business rules to drive segmentation**
  Define your segmentation strategy according to your business goals.

  For example, you might segment by income in order to target a more affluent audience; or you might segment by age range if you want to develop your next generation of brand advocates.

- **Define segmentation against campaign goals**
  If you are pursuing more immediate campaign goals, look to the product or service you are promoting to identify segmentation criteria.

  For example, if you are selling a range of different holidays then you might want to segment according to multiple criteria – such as by income, if promoting budget or premium breaks; or by number of children, if promoting holidays for either families or couples-only.

- **Adapt marketing to groups**
  Segmentation gives you huge opportunities to adapt your marketing communications to appeal to the specific characteristics of each customer.

  For example, you might identify and segment all 30-40 year-old women who have spent over £50 with you in the last six months – and send them a particular offer to them that you know will be highly relevant, welcomed, successful and cost-effective.

Data usage

- **Develop specific strategies for different groups – put your customer first**
  As with all one-to-one marketing, put yourself in the mindset of your customer.

  Do this for each segment to devise the most compelling message and delivery method for each group – and enjoy the fullest rewards from your marketing.

- **De-dupe before campaign**
  It is possible that an individual customer might appear in multiple segments, especially if you are sending a campaign to groups defined by different criteria – for example, a certain age group PLUS a certain income band PLUS a certain buying behaviour.

  Therefore you MUST de-duplicate your data before you run your campaign in order to minimise the chance of your customer receiving your message multiple times.

- **Screen and suppress before sending**
  Screen your segmented data against all appropriate in-house, DMA and industry suppression files before processing or using it.

- **Keep records of selection criteria**
  Keep documented records of the selection criteria you use for a campaign for a minimum of one year.

Static selection

- **Static selections are pre-set data groups**
  Static selections are the criteria by which you decide to group your data.

  For example, you might prefer to group age ranges as 18-24, 25-34, 35-44, and so on; alternatively, it might suit your business needs more appropriately to group as 18-30, 31-50, 50+.

- **Use static selections to pre-set segments**
  Once you have profiled and segmented your data and understand how best to define each customer group, set up your 'static selections' to define these segments consistently across your marketing teams and campaigns.

- **Set up to give targeting power and efficiency**
  By filtering customer records into the right groups, you can combine static selections to efficiently target ideal customers on a campaign-by-campaign basis.

  For example, you might want to respond to a topical event by promoting an offer on a relevant product to 25-34 year-old women with children and a household income over £40,000.

  By having static selections already defined for each of these criteria, you will be able to pull all of these customers out of your database quickly and easily during a campaign.

- **Use to pre-check consent**
  Set up your static selections to pre-check each customer for consent, communication preferences and suppression files and filter out inappropriate records before your campaign team needs to handle them.

- **Use static selections to automate marketing**
  You can use static selections to set up automated marketing that is triggered by a customer's actions – for example, looking at a particular product – or to include appropriate messages in service communications.

Real-time and dynamic targeting

- **Automate real-time segmentation**
  You can seize the opportunities of real-time, dynamic targeting by setting up a system to automatically move each customer into the most appropriate segment according to their behaviour.
- **Use real-time segmentation to optimise data**
  This allows you to keep your data up to date and more valuable – as your customer might regularly move into different segments as their conditions change.

  For example, your customer's actions on your website might indicate a change in their circumstances – such as more income, less income, having children or being in the market for a new type of product – allowing you to respond with appropriate marketing messages.

  You might also want to automatically re-categorise your customer into a different segment if they request more information on a certain product, share your content on social media or you detect via their mobile device that they are currently within the vicinity of your retail outlet.
- **Automate responsive one-to-one marketing**
  Set your system to automatically identify the next action for this customer, when to execute it and via which channel.

  For example, if you pick up from their mobile that your customer is near your retail outlet, your system might immediately send them an SMS discount voucher valid for the next hour.
- **Monitor real-time systems to ensure appropriate, effective use**
  It is critical that you monitor your dynamic systems constantly to make sure that they are operating within appropriate boundaries and that your customers are responding to your marketing positively and as expected.

Metrics and reporting

Strategy

- **Use metrics to measure campaigns**
  Metrics are a powerful tool in your undertanding of how, when and why your campaign is performing.
- **Align metrics to goals**
  There are many metrics available and it is important to choose the right ones in order to keep your marketing aligned to your business objectives and other marketing activity.

  Choosing the wrong metrics can cloud rather than inform your understanding of how a campaign is performing – and be a costly and potentially irretrievable error to discover after your campaign has launched.
- **Identify different analytics needs**
  Different functions within your organisation will need different analytics to help them improve.

  This is true whether you are working for a multi-national corporation or running your own small business – different metrics will inform different processes.

  Identify simple, suitable metrics for each of your core needs – for example:
    - Specific campaign performance
    - Overall performance trends
    - Operations
    - Website performance
    - Brand reputation
    - Market share
    - Customer service
    - Product competitiveness
    - Competitor analysis
- **Measure for trust and reputation**
  Do not be misled into judging your success simply on 'Likes' and followers – these can be bought easily and cheaply, regardless of how relevant your marketing is, and could just represent a large audience of expensive and poor-quality prospects.

  Instead, identify metrics – particularly over the longer term – that will give you a true sense of your standing within your target audiences. Do they engage with you beyond your marketing? Do they look to your brand as an authority in your sector? Do they come back more than once? Do they advocate you to others?
- **Be selective**
  These days, pretty much everything can be measured. A vast amount of information will be easily available to you through analytics attached to all sorts of applications – but most of these will not be useful enough to your specific needs to make them worth investing time or resource into.

  Make sure that you concentrate on the particular metrics – or combinations of metrics – that you know how to make meaningful use of.
- **Build analytics in at planning stage**
  Make sure you carefully consider all options and build these measurements into your campaign from the planning stage.

If you try to include analytics later on, it may be too late to build them into your systems effectively or efficiently and could undermine your efforts to understand your marketing.

- **Assess channel performance**
  If a campaign is not working, do not automatically discredit the channel as ineffective for your needs.

  The success of marketing on ANY channel is dependent on many factors – strategy, creative, relevance, timing, quality of execution and delivery.

  Isolate the impact of other factors and be sure that it is the specific channel that is ineffective before writing it off.

- **Measure ongoing performance**
  Measure ongoing performance, not just individual campaigns.

  Individual campaigns may well perform unusually strongly or weakly, often for no clear reason, so it is vital to track performance over all channels on an ongoing basis.

  Only this way will you be able to identify the significant moments or general trends in your marketing that can underpin your successful future business and campaign strategies.

- **Assign your analytics expert**
  No matter how small your organisation, it almost certainly will be invaluable to nominate one member of your team to 'own' your analytics.

  Give them the scheduled time and resources to truly understand what analytics are available and appropriate, and charge them with the responsibility to monitor your business and campaign performance and to make meaningful reports to key stakeholders that can lead to performance uplifts.