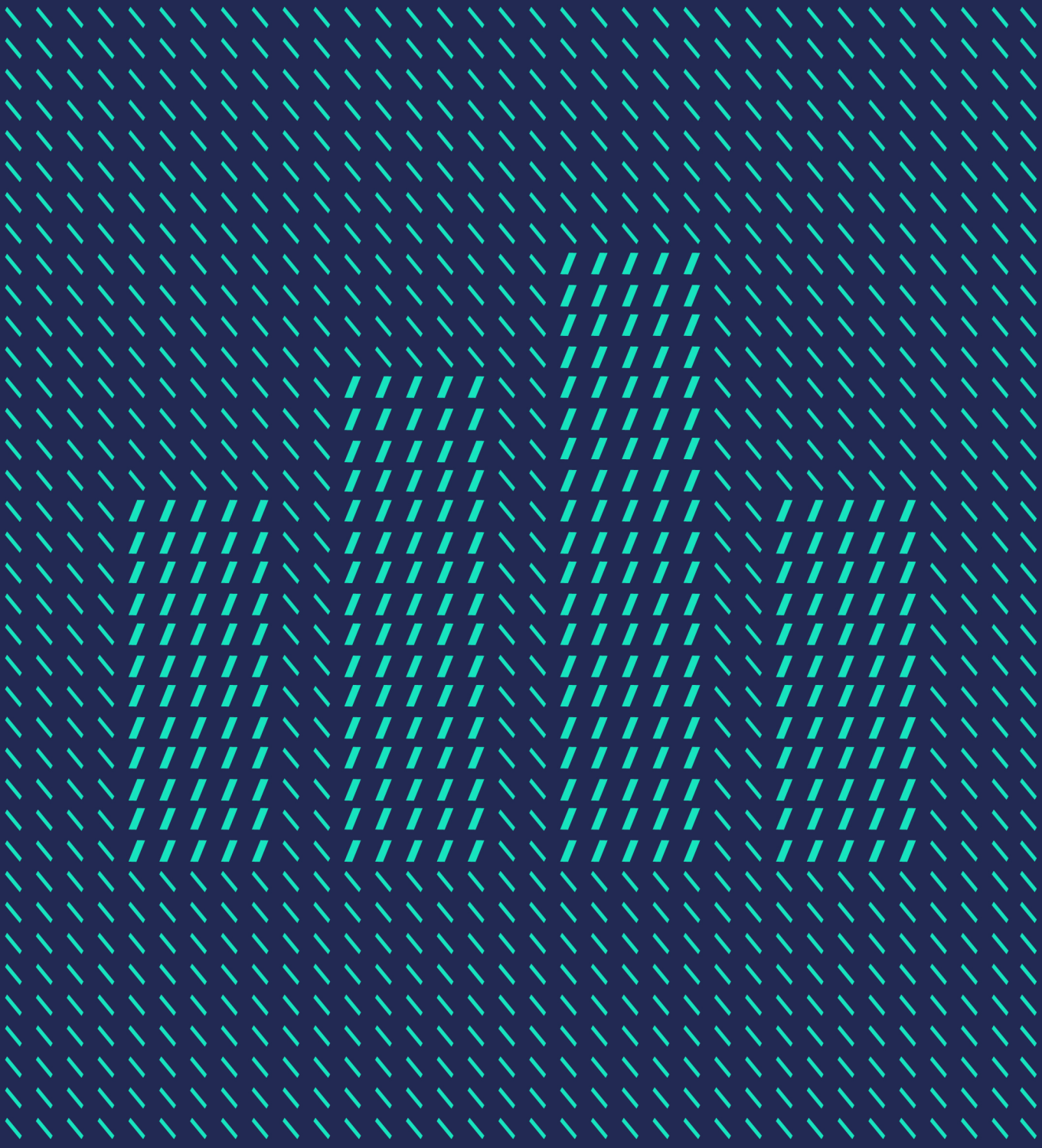
Data Guide

DMA
Data & Marketing Association



Contents

Copyright / DMA (2019)

Copyright / DMA (2019)

Introduction

Legislation

Data legislation is designed to protect the rights of the consumer and ensure that any personal data held or used is processed fairly and lawfully.

Data availability and use for marketing are 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 out the UK legislation website here to keep up to date with latest amendments for these and all other legislation.

Data Protection Act 2018 (DPA 2018)

The Data Protection Act 2018 came into force on the 25 May 2018, ushering in a new era of personal data regulation in the UK. The Act supplements the much-anticipated EU General Data Protection Regulation (GDPR) and incorporates it into UK law.

The GDPR and DPA 2018 are the key legislation governing your one-to-one marketing activity.

They have two main aims:

- To protect the rights of the individual.
- To ensure that any data processed is necessary for that processing, has been fairly and lawfully collected, is kept securely and is accurate and up to date where necessary.

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)

Copyright / DMA (2019)

Business Practice

Business Practice

The Six Principles of the GDPR

The GDPR outlines six 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.

Underlying all of these principles is accountability for controllers and processors. This principle requires you to be able to provide evidence that you comply with the principles of GDPR. The process of accountability is about having in place all of the policies and documentation necessary to demonstrate that what you are doing with personal; data is fair and compliant and considers the right of individuals.

For further details on accountability click here

1. **Transparency**
   Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. **Purpose limitation**
   Personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. **Data minimisation**
   Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy**
   Personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Storage limitation**
   Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals

Copyright / DMA (2019)

6. Integrity and confidentiality

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Copyright / DMA (2019)

Business Practice

Your Obligations

You must have a valid legal basis in order to process personal data. There are six legal bases, and the most appropriate one to use depends on the purpose of the processing.

You must determine the legal basis for processing before the processing takes place. This should be documented and captured in publicly available privacy policies and notices.

You are not able to switch between legal bases without good reason, so it is important to consider this and get it right first time.

Legal Bases:

- **Consent**
  Consent is just one of the legal bases for processing data.

  You need consent to use an individual's data for marketing via email or text or automated calls and explicit consent when processing special categories of data. Consent must be unambiguous and involve a clear affirmative action. The GDPR bans pre-ticked consent boxes. It also requires distinct granular consent options for distinct processing operations.

  If you are offering online services to children and want to rely on consent for your processing, you need to adopt age-verification measures and seek parental consent for children under 13 (UK law – ages differ per EU country).

  Consent should be separate from other terms and conditions and should not be a precondition of signing up to a service.

- **Legitimate interest**
  Where you do not have to gain consent for marketing, legitimate interests may be a valid legal basis. You can only rely on legitimate interest where the rights and freedoms of the individual, whose personal data will be processed, has been evaluated and these interests do not override the controllers' legitimate interest

  For further details on consent and legitimate interest, click here.

  Further details on the additional legal bases – Contract, Legal Obligation, Vital Interests or Public Interest – can be found here.

- **Define policies**
  Maintain clear policies and processes.

- **Stated use**
  Only use data for the purpose for which it is provided.

Copyright / DMA (2019)

- **Honour customer preferences**
  Honour each customer's data preferences.

- **Accuracy**
  Ensure that any data held is accurate where necessary.

- **Up-to-date**
  Ensure that any data you use for marketing purposes is up to date.

- **Assign data responsibility**
  Assign clear responsibility for data within your organisation.

- **Security**
  Ensure appropriate data security.

- **Staff training**
  Train your staff to handle data appropriately.

Copyright / DMA (2019)

Business Practice

Penalties for Non-compliance

Besides the power to impose fines, the **ICO** has a range of corrective powers and sanctions to enforce the GDPR and DPA 2018. These include issuing warnings and reprimands (these can be public which can result in reputational damage and loss of consumer trust); imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive".

There are two tiers of administrative fines that can be levied:

1. Up to €10 million, or 2% annual global turnover – whichever is higher
2. Up to €20 million, or 4% annual global turnover – whichever is higher

The fines are based on the specific articles of the GDPR that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

When deciding whether to impose a fine and the level, the **ICO** will consider:

- The nature, gravity and duration of the infringement
- The intentional or negligent character of the infringement
- Any action taken by the organisation to mitigate the damage suffered by individuals
- Technical and organisational measures that have been implemented by the organisation
- Any previous infringements by the organisation or data processor
- The degree of cooperation with the regulator to remedy the infringement
- The types of personal data involved
- The way the regulator found out about the infringement
- The manner in which the infringement became known to the supervisory authority, in particular, whether and to what extent the organisation notified the infringement
- Whether, and, if so, to what extent, the controller or processor notified the infringement
- Adherence to approved codes of conduct or certification schemes.
- The GDPR also gives individuals the right to compensation of any material and/or non-material damages resulting from infringement. In certain cases, not-for-profit bodies can bring representative action on behalf of individuals. This opens the door for mass claims in cases of large-scale infringements.

Copyright / DMA (2019)

Data Acquisition

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 data to feed your campaigns. Using the correct data 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 consider the nature of your product and customer relationship.

- **Follow data protection by design**
  Map out the data flow through your organisation. Ensure you are following the key principles (see the section The six principles of the GDPR in this guide) and check appropriate security measures are in place to keep data safe.

- **Research, test and understand**
  Research, test and understand the most important drivers of marketing permission for your customers. Younger and older audiences will share concerns over data security and over contact but their wants and needs will be very different in terms of giving their data in exchange for better experiences from you.

- **Ask for the bare minimum you need**
  The less data you ask for, the more likely your customer is to share. Do not ask for data for the sake of it – any data will cost you money to process and will affect your customer's expectations of you. Do not forget that principle three of the GDPR states that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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 data at relevant moments – such as in-store, at a relevant event or during targeted marketing activities.

Copyright / DMA (2019)

- **Time your request**
  Ask for data at the point at which it is most appropriate.

  For example, you might ask for data while your customer is using your product; or schedule further data gathering for relevant points in your customer lifecycle.

- **Split your data capture into relevant stages**
  You can always ask for further data at more appropriate opportunities, later in your customer lifecycle.

Logistics

- **Record all data clearly, accurately, and in an accessible and usable way**
  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.

Copyright / DMA (2019)

Data Acquisition

Legal Basis

Permission to use Personal Data

Remember, you must have a valid legal basis for processing personal data. Once you decide on your legal basis, you must stick to it.

- **Gaining consent before marketing**
  If using consent, you need to review your consent mechanisms to make sure they meet requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn. For further details click here

- **Or relying on legitimate interest**
  You need to carry out a legitimate assessment if you want to use this for processing for a particular purpose. For further details click here

- **Meet your industry code obligations**
  It is your legal obligation under the GDPR, DPA 2018 and the PECR to gain marketing permission – and a condition of all relevant industry codes and standards, including the DMA Code and the CAP Code.

- **Safeguard against negative customer reaction**
  Your customers are much more aware of privacy and data issues than ever be-fore 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 permission to do so.

- **Improving customer relationships**
  More positively, both gaining unambiguous consent or performing an assessment to balance legitimate interests enables you to give your customer relevant and engaging 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 wel-come it.

Copyright / DMA (2019)

Data Acquisition

Additional Obligations to your Customer at Sign-up

- **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.

- **Declare any third-party usage**
  You must explain if your customer's data is to be used for your own marketing or passed to third parties for marketing purposes.

  If relying on consent, you should name third parties with whom you share data. If relying on legitimate interests, you must provide details about the industry categories of the third parties. For further details, click here.

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

Copyright / DMA (2019)

Data Acquisition

Channel-specific Consent Rules

Email and SMS

Consent

The general rule under PECR is that you need consent from an individual to receive marketing communications by email and SMS.

- **Higher threshold for digital**
  PECR requires consent for collecting and using data for marketing in electronic channels.

Soft Opt-in

- **Specific to email and SMS marketing**
  There is an exemption in PECR, the soft opt-in, which allows you to conduct one-to-one marketing on the basis of offering an opt-out (legitimate interests) 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**
  Charities can only use soft opt-in for their trading arms, not for fundraising.
- **Collect channel-specific opt-ins**
  You must collect specific permissions for each marketing channel.

Copyright / DMA (2019)

Telemarketing

Opt-out

- **Telemarketing is currently opt-out**
  Telemarketing is currently permitted on an opt-out basis (though if relying on an opt-out you do need to have run your legitimate interest assessment before going down this route). However, it is a legal requirement that all organisations (including charities, voluntary organisations and political parties) do not make such calls to numbers registered on the TPS unless you have an individual's consent to do so.

Sourcing Phone 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 – UNLESS you have gained the individual's consent to call.

Direct Mail

Consent

- **Higher threshold under GDPR**
  The GDPR requires that consent is unambiguous, shown by a clear opt-in such as ticking a box and that individuals are fully informed as to why and how their data will be used. You also need to offer the opportunity to unsubscribe and this should be made as easy as providing consent in the first place.

Opt-out

- **Offering an opt-out**
  If you are using legitimate interests as your lawful basis, you must offer the ability to opt-out at the point of data capture and on all subsequent communications. Opting-out must be as easy as it was to provide permission in the first instance.

Copyright / DMA (2019)

Best Practice Guidelines Across All Channels

Best Practice Guidelines Across All Channels

Opt-out

- **Right to opt-out**
  Individuals have an absolute right to stop their data being used for direct marketing. You must tell individuals about their right to opt-out. An individual can make an objection verbally or in writing and you have one calendar month to respond to an objection. For further information, click here

  Mail Preference Service (MPS) enables consumers to opt-out of unsolicited personally addressed mail. It is not a legal requirement to screen against MPS but it is best practice to respect consumers wishes and it is also a condition of the DMA membership to screen against the MPS file.

- **Add consumers to an 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.

  A separate record should also be used for the right to restrict processing requests (individuals have the right to request the restrict the processing of their personal data – click here) and for the right for erasure request (also referred to as the right to be forgotten – click here).

- **Charity-specific screening**
  The Fundraising Preference Service (FPS) allows people to control how charities contact them through either reducing the frequency or opting-out entirely. If you are a charitable organisation, you must screen against this service.

- **Use the most recent instruction**
  In all cases, it is the most recent piece of information or instruction received from your customer that takes priority.

Permission Statements

- **Template statements**
  Use the DMA consent and legitimate interest statement builder to create statements specific to your needs. You can find the template here.

Copyright / DMA (2019)

Privacy and Data Protection Notices

Privacy and Data Protection Notices

There is a requirement for transparency at the point of data collection regarding your likely future uses of your customer's data. It is important that information about who you are and what you want to use the data for is given at this point.

Other data protection information can be provided elsewhere by way of a clear and easy-to-understand privacy policy, which should be hyperlinked from the data collection statement.

Copyright / DMA (2019)

Privacy and Data Protection Notices

Strategy

- **Ensure compliance**
  Ensure your privacy policy is compliant with the law. For further guidance, click here.

- **Consult the DMA**
  The DMA can provide advice on what it should contain but it is your responsibility to ensure all processing is covered under the privacy policy and that it is compliant.

- **Use the privacy statement as a relationship opportunity**
  Under the DPA your privacy policy cannot be a long passage of impenetrable legal jargon.

A good privacy policy 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 your 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, but ensure it is still legally accurate.

- **Include the link to the 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 notice on 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.

Copyright / DMA (2019)

- **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.

Copyright / DMA (2019)

Privacy and Data Protection Notices

Content

- **Layer it**
  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 legalcompliance.

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

- **Tailor your 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**
  Click here for the privacy policy template.

Copyright / DMA (2019)

/ Cookies & Similar Technologies

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

You must tell people if you set cookies, and clearly explain what the cookies do and why. You must decide on your lawful basis for using cookies. You will be able to use different lawful bases for different cookies if they have different purposes.

For cookies that are essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking), you should be able to use 'in connection with a contract', but the more intrusive the cookie, the more likely you would need to gain consent from the individuals.

The same rules also apply if you use any other type of technology to store or gain access to information on someone's device

Cookie Consent

There are all various subtleties around how you ask for consent 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 of 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.

Copyright / DMA (2019)

Cookie Stakeholders

- **Assign board-level responsibility**
  Assign someone at board level to ensure your cookie management is 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 web managers**
  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 of 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:

Copyright / DMA (2019)

- 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 Permission for Cookies

Not all cookies are used in a way that could identify users, but the majority are and will be subject to the legislation. This includes cookies for analytics, advertising and functional services, such as survey and chat tools.

To become compliant, organisations will need to either stop using cookies or find a legal basis to collect and process that data. Further information can be found here.

If you need/decide to use consent, you need to decide how you will obtain this from users of your site(s).

Methods include:

- Pop-up boxes
- Splash pages
- Landing pages
- Homepage headers
- Banners
- Scrolling text
- Tick boxes

Copyright / DMA (2019)

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.

If using Consent for Cookies

- Implied consent is no longer going to be compliant. There are several reasons for this. Mainly it's because GDPR consent requires the user to make an 'affirmative action' to signal their consent. Simply visiting a site for the first time would not qualify. So loading up your landing pages with cookies in the hope people won't opt-out, won't wash.
- Advice to adjust browser settings won't be enough. It must be as easy to withdraw consent as give it. Telling people to block cookies if they don't consent would not meet these criteria.
- By using this site, you accept cookies' statements will not be compliant. If there is no genuine and free choice, then there is no valid consent.
- Sites will need a way to withdraw consent. Even after getting valid consent, there must be a route for people to change their mind. Again, this comes down to the requirement that withdrawing consent must be as easy as giving it.
- You need a response to 'Do Not Track' browser requests. A DNT:1 signal is a valid browser setting for communicating a visitor preference. It could also be interpreted by regulators as an exercise of the right to object to profiling.
- Consent will need to be specific to different cookie purposes. Sites that use different types of cookies with different processing purposes will need valid consent mechanisms for each purpose. This means granular levels of control, with separate consents for tracking and analytics cookies.

Copyright / DMA (2019)

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 marketing permission 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
    - What legal basis are you using for each cookie
    - Expiry / retention period
    - How your user can give and withdraw consent
    - How can the user opt-out if you are using legitimate interests?

- **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 the 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**

Copyright / DMA (2019)

Data Sources

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, but remember to tell your customers that you will do this..

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

Copyright / DMA (2019)

- **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**
  While 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 the 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. You need to decide which lawful basis you will use to gain permission for marketing purposes.

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.

- **Capture marketing permission per channel**
  Once you have your lawful basis, you need to provide the correct data capture

Copyright / DMA (2019)

statement, so for opt-in if using consent and opt-out if using legitimate interests. Permission should be gained for each channel you wish to use.

- **Record permissions gained**
  You should record against the individual's details the marketing permissions you have gained.

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, here.

Copyright / DMA (2019)

Asking Consumers to Refer Friends and Family

Asking Consumers to Refer Friends and Family

When thinking about any marketing route, most importantly you must still comply with the GDPR and act transparently and fairly. You cannot avoid your legal obligations by asking existing contacts to provide contact details for their friends and family; you must act in the best interests of the individual – you cannot assume that the referrer has taken them into account.

The **ICO** does not endorse this type of referral marketing, as it is difficult to be sure there is the necessary demonstrable consent to comply with the law.

If you do wish to undertake a referral campaign, seek advice first. You will be recommended to clearly explain that the referrer should only provide someone else's details with that person's informed consent and that the person will be told who provided their details. This may fulfil the GDPR principles of lawfulness and transparency. At the first opportunity, you need to provide a privacy notice to the new contact as soon as possible (unless it would be disproportionate to do so).

Copyright / DMA (2019)

Third-party Data

Third-party Data

Since the introduction of the new data legislation, there have been myths and misconceptions about the use of third-party data, with marketers questioning the feasibility of using third-party data to find new customers.

There is nothing in the GDPR that prohibits the use of third-party data, provided that it is approached and undertaken in the right way with the appropriate safeguards.

For more information, please see the Third-Party Data Guide, here.

Copyright / DMA (2019)

Data Removal

Data Removal

Unsubscribe Requests

Individuals have the right to unsubscribe from marketing communications. Organisations must tell individuals about this right

- **Identify the scope of the 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 and set the customer's expectations.

- **Action**
  Action as soon as possible, depending on the channel.

- **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.

- **Further Information**
  Further information on how to respond and action requests can be found in specific channel guides, available here.

Copyright / DMA (2019)

Withdrawal of Consent

Withdrawal of Consent

Individuals have the right to withdraw their consent to processing and organisations need to tell individuals of this right and make it as easy to withdraw as it was initially to give consent.

Copyright / DMA (2019)

Data Subject Rights

Data Subject Rights

The GDPR builds upon and strengthens some of the rights of individuals laid down under previous law, as well as introducing new rights.

These rights are:

- The right to be informed
- The right of access (where individuals can make a Subject Access Request)
- The right to rectification
- The right to erasure (known as “the right to be forgotten”)
- The right to restrict processing
- The right to data portability
- The right to object

Rights in Relation to Automated Decision Making and Profiling

Organisations processing data must now adhere to strict response time limits and – unless circumstances apply – cannot apply a fee to individuals exercising these rights.

Both individuals and organisations must understand that there are exemptions and circumstances when these rights cannot be exercised or applied.

For more information on Individual Rights, including your obligations and how to respond, see the ICO’s extensive guidance on Individual Rights, here.

See also the DMA GDPR resources including the DMA GDPR guidance: Profiling, here, for more details.

Copyright / DMA (2019)

/ Data Care

Data Care

Data Hygiene

It is inevitable that data will start to decay as soon as it is collected, as individuals' circumstances change. Constant maintenance is key.

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

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 data such as date of birth or financial status, which individuals believe to be sensitive.

  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.

Copyright / DMA (2019)

Data Protection Principles

- **Adequate and not excessive**
  You should only collect and maintain adequate data required to perform the processing. Excessive and unnecessary data is not permitted under the GDPR.

- **Accurate and up-to-date**
  It is a legal requirement under 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 GDPR states that personal data is "that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

Screening and Suppression

Screening your lists for gone-aways, deceased people and opted-out customers enables you to only use accurate, effective and up-to-date data.

It is an obligation under the GDPR, the DPA 2018, the DMA code and the CAP Code to screen your lists.

Suppression Files

Suppression files are records of individuals who have objected to marketing.

- **Suppression files can include:**
  - People who have unsubscribed or said do not mail
  - Individuals who have altered their communication preferences

Other file types should be collated and used to ensure that data is always kept accurate and up to date.

- **Update files:**
  - Gone-aways – customers who have moved address and haven't notified you of their new details
  - Deceased people
  - Credit risks

Copyright / DMA (2019)

- **Information contained in both business suppression and update 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

For more information on screening, see our Advertising mail and marketing guide, the Telemarketing guide, the Mobile guide and the Email guide, all available here.

Copyright / DMA (2019)

DMA Preference Services

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)

Copyright / DMA (2019)

/ Telephone

Telephone

It is unlawful to make a call to an individual who has indicated that they do not wish to receive such calls – whether they have registered with TPS or notified your organisation directly.

Copyright / DMA (2019)

Telephone Preference Service (TPS)

Telephone Preference Service

About TPS

- **Consumer telemarketing opt-out**

  The TPS is a list of 20.5million consumers (May 2018) who have registered their telephone numbers in order to stop receiving unsolicited live telephone marketing calls. Registration covers the consumer as both a private individual and as a sole trader or involved in a business partnership – so you must screen against TPS when conducting business-to-business calls as well as business-to-consumer ones.

  www.tpsonline.org.uk

Your obligations under TPS:

- **Comply with PECR**
  The current legislation governing the TPS is PECR.

  If you make unsolicited marketing telephone calls to individuals, you must comply with PECR. This also applies if you work for a charity, voluntary organisation, political party or any business.

Find out more
For more information, see our *Telemarketing guide*, here.

Corporate Telephone Preference Service (CTPS)

- **Corporate telemarketing opt-out**
  The CTPS is run in the same way as the TPS, which 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.

- **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.

Copyright / DMA (2019)

/ Direct Mail

Direct Mail

Mailing Preference Service (MPS)

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

- **Compliance and the 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. There is no legal requirement to use MPS against your existing in-house customer files.

Find out more
For more information, see our *Advertising mail and marketing guide*, here.

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

Copyright / DMA (2019)

/ Fax

Fax

Facsimile Preference Service (FPS)

The FPS File is a of individuals and businesses that object to receiving unsolicited marketing faxes. expressed a wish to opt-out of receiving unsolicited, 'cold' advertising mail and is governed under PECR.

- **Do not Fax FPD registrants**
  It is unlawful to send a fax to an individual unless you have their prior consent. The term 'individual' in the UK law includes consumers, sole traders and partnerships (except in Scotland).

- **Find out more**
  See www.fpsonline.org.uk/ for more information.

Copyright / DMA (2019)

About the Campaign

About the Campaign

Responsible Marketing

Changes to the governance of data have far-reaching consequences for your business.

The new General Data Protection Regulations (GDPR) has already had an effect on how your business does business, and how it manages, protects and administers data in the future.

The new regulations came into place in 2018 and are still making waves.

At the DMA, we want to demystify these regulations and offer support to help you work to the best of your ability.

We also run events to encourage the practice of Responsible Marketing. Our popular Legal Updates discuss the current political and legal affairs affecting the industry and allow you to speak directly with the DMA's finest legal minds. Keep an eye on your emails, or visit our events page to book your spot.

For those dealing with vulnerable consumers, we have a masterclass in recognising the needs of vulnerable consumers and how to make reasonable adjustments to benefit a broad range of employees working with customers in vulnerable circumstances.

Find help and guidance for all matters regarding responsible marketing on the DMA site.

Copyright / DMA (2019)

About the DMA

About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should be done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focussed principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

Copyright / DMA (2019)

Copyright and Disclaimer

Copyright and Disclaimer

‘DMA Data Guide: Best Practice’ is published by the Data & Marketing Association (UK) Ltd Copyright © Data & Marketing Association (DMA). All rights reserved. No part of this publication may be reproduced, copied or transmitted in any form or by any means, or stored in a retrieval system of any nature, without the prior permissionof the DMA (UK) Ltd except as permitted by the provisions of the Copyright, Designsand Patents Act 1988 and related legislation. Application for permission to reproduceall or part of the Copyright material shall be made to the DMA (UK) Ltd, DMA House,70 Margaret Street, London, W1W 8SS.

Although the greatest care has been taken in the preparation and compilation of ‘DMA Data Guide: Best Practice’, no liability or responsibility of any kind (to the extent permitted by law), including responsibility for negligence, is accepted by the DMA,its servants or agents. All information gathered is believed correct at June 2019. All corrections should be sent to the DMA for future editions.

Copyright / DMA (2019)