DMA advice: Using third party data under the GDPR

Contents

Introduction

Since GDPR was on the drawing board, there have been myths and misconceptions about the use of third party data.

Throughout the world of marketing suggestions have pervaded that the ability of organisations to use third party data to find new customers or to understand existing customers better in order to offer them a more relevant marketing experience, is challenging, if not impossible, under the GDPR.

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

For many organisations third party data provides them with significant opportunities to engage with consumers in a relevant and appropriate way:

- 3Providing support, insight and market context to grow their customer base
- To develop appropriate products and services for their marketplace
- To provide relevant and appropriate marketing experiences to existing and potential customers

This DMA advice document outlines the importance and on-going use of third party data for marketing under the GDPR.

It will outline how third party data may be used in the context of the GDPR to assist organisations in their marketing activities through looking at the use of third party data across three areas of marketing activity:

- Prospect or contact marketing
- Analytics, segmentation and data enrichment
- Linkage and data quality services

The primary focus is to outline these three high level third party data use cases, predominantly around offline third party data.

Whilst we reference the value these can add through digital channels, it isn't meant to be exhaustive around digital applications.

This landscape is complex and changing all the time with the ePrivacy final draft yet to come. A future version may add more digital use cases, post-ePrivacy final draft.

However, to set the context, we need to explain what we mean by third party data and how is this different from first (and second) party data. In doing so, we highlight the benefits that compliant, high quality third party data can bring to an organisation's marketing activities in the best interest of the consumer.

It's logical to start by looking at first party data so that you can see how third party data works with an organisation's own data to increase the power and efficiency of your marketing.

Acknowledgments

Paul Cresswell	***Experian***
Paul Winters	***CACI***
Michele Masnaghetti	***Abacus Epsilon***
Andrew Bridges	***The REaD Group***
Jonathan Carter	***Acxiom***
Nicholas McCarthy	***Merkle***
Tim Roe	***Red Eye***

Before reading this advice

It is important to remember that this document provides general advice for the majority of common marketing scenarios. It does not remove an organisations responsibility for doing their own data protection impact assessment (DPIA), their own legitimate interest assessment (LIA), or any other aspect of GDPR compliance. All of the advice needs to be viewed in context, and the outcome of the assessments may be different from company to company. Each organisation will have to satisfy itself that it has a valid legal ground to process the data as they want to and they should be confident that the suppliers of third party data have done the same.

At the time of writing this advice we are not aware of any other guidance available on the practical use of third party data in marketing. This is probably because third party data is a very broad and highly complex subject with potentially far reaching implications throughout the industry. It would be almost impossible to create guidance that accurately covered all aspects of third party data use, so we have decided to start with the basics that form the foundation of much of the direct marketing that goes on. This document should be seen as a starting point for discussion and something that can be expanded on, updated and corrected as new guidance, case law and legal opinions come to light.

To keep the advice to a manageable size we have not expanded on complex subjects covered by other guidance documents, nor have we included large sections of the GDPR articles or recitals. We have instead referenced these with links to other material. For example, where the advice might say "appropriately permissioned third party data" we do not go on to explain how that permission should have been collected as all data sources are different and each case needs to be judged on its own merit. Where such examples exist, we will include a link to the relevant guidance on this subject.

The advice does not cover the more complex issues of special category data or the affect that marketing related to a more sensitive or contentious subject such as products like alcohol and tobacco, political campaigning, or targeting particular life stages such as expectant mothers all of which require more cautious consideration.

The impact on the consumer should always be the priority consideration. When weighing up whether or not legitimate interest is the right legal ground for processing data the ICO's legitimate interest guidance or the DMA's Consent and Legitimate Interest guidance should be consulted and a legitimate interest assessment completed and recorded. The three elements of which are:

- Identify a legitimate interest;
- Show that the processing is necessary to achieve it; and
- Balance it against the individual's interests, rights and freedoms

Any processing of personal data should be done in line with the GDPR.

What is first party data?

Nobody knows your customers like you do.

First-party data is information you have collected directly from your own customers — data about users and their interactions directly with your brand that you get by tracking your own relationship with that customer.

Examples include:

- Website registration data
- Online purchase information for customers
- In-store purchase information from a loyalty card/program
- PC, mobile and in-app web browsing, location and behaviour data
- Records of email
- Campaign performance data

It's easy to see why this is powerful: it's what fuels the deeper, more intimate relationships that lead to brand advocacy, long-term customer commitment and higher revenue and margins.

Use of first party data is not without its challenges, particularly around the collecting and storing this data at volume.

The collection of data should always be carried out in compliance with data protection regulations, most significantly it should be fair, transparent and lawful. If you are collecting personal data from your own customers, some of the things you have to think about under GDPR are the same as those for any type of data – first, second or third:

- Making sure you have the appropriate consents or permissions from your customers to enable your particular marketing use cases.
- Ensuring the quality and accuracy of the data.
- Having appropriate data retention and minimisation policies.
- Ensuring the security of the customers' data.
- Ensuring transparency to consumers around how you are going to use that data.

What is second party data?

Perhaps the "new kid on the block", you may hear the term "second party data" as organisations begin to form strategic partnerships and affiliations to share information.

Second party data is a specific sub type of third party data; it is someone else's first party data that you have permission to use as part of a closed group agreement e.g. between two brands.

It is first party data from another source if you like – meaning it's collected in the same manner as first party data. However, that data is then shared with another organisation for a limited set of purposes.

The data collected by the partner needs to be collected and used in accordance with the requirements of GDPR including ensuring that there are appropriate permissions in place to share the data and the appropriate privacy information has been supplied.

What is third party data?

Third party data is not typically from a single source, rather a consolidation of data (both personal data and non-personal data) across a set of sources and licensed to third parties, often for use in data analysis and targeting for marketing purposes.

That third party may have collected the data direct from the individuals or obtained them from a variety of other sources, including publicly available registers. It is important to remember that just because personal data is publicly accessible it does not mean that it can be used without following the relevant legislations. It still needs to be processed in accordance with the requirements of GDPR to ensure that the use is fair and within the reasonable expectations of the data subject.

Third party data includes two broad categories of data:

1. Listings of identities, together with links to contact details and history for each, across a wide range of channels.

   Examples include:

   - Contact data – current and past name, postal address, email address, telephone number
   - Online identifiers – cookies, IP address, browser type and mobile device identifiers

2. Attributes for each identity, describing demographics, behaviours and attitudes using a mix of actual and modelled data available at varying levels of granularity such as postcode, household or individual level.

   Examples might include:

   - Age
   - Gender
   - Hobbies
   - Purchasing behaviour
   - Segmentations
   - Life events - individuals who have recently moved home or had a baby

What kinds of organisations offer third party data for marketing?

Marketing services organisations and data management businesses often bring together personal data (such as name and address) from offline and online sources into a third party marketing database.

This data may, subject to ensuring the requirements of GDPR and PECR are met, be used for contact purposes (e.g. for email or postal direct marketing to prospects) and for linking other information to your own customer data.

This third-party data is often sourced from trusted data partners who have direct contact with the data subject already, and where appropriate permission has been obtained from the data subject and / or notice has been given for them to pass your information to third parties for use in creating marketing products and services.

These sources might include:

- From public data sets, for example, the edited version of the Electoral Register (EER)
- Collected direct from consumers, particularly for marketing purposes, often referred to as "lifestyle lists/ surveys", "prospect files" or "lead generation lists"
- Subscription files from publishers (names and addresses of subscribers to various publications, publisher sites, and money saving / offer websites
- Pooled databases of consumer names and addresses (e.g. a data cooperative where a group of companies share the names and addresses of their customers with appropriate permissions, such as a mail order cooperative)
- Online data capture, data captured from apps on mobile phones or behaviours from users on websites

These same third party marketing data providers often offer analytical models and segmentations to their clients, perhaps created using market research data and other aggregated information from multiple sources to model likely consumer behaviours and to create consumer segments (often referred to as "audiences") for targeting ads and marketing communications.

Some data-management and marketing services businesses offer lead generation services to organisations whereby they collect appropriately permissioned personal data for use by that organisation (and by others if the consumer has agreed to this).This might include lists of consumers who have expressed an actual interest in being contacted about a particular product, offer or service (as opposed to the models discussed above which infer the likely behaviours or interest of an individual).

References and further reading

DMA Guidance on Consent and legitimate interests

https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

ICO Guidance on Consent

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO Guidance on Legitimate Interests

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Can third party data be used for marketing purposes under the GDPR?

We've already made clear that there is nothing in the GDPR that prohibits the use of third party data, provided that it is undertaken in accordance with the data protection principles and regulatory guidance.

Rather the GDPR seeks to ensure that, through its key transparency and accountability principles, organisations are building an environment where consumers can understand and control what is happening with their personal data, what it is being used for and by whom.

Assuming that transparency, control, and other safeguards are in place and that all organisations have an appropriate lawful ground for processing personal data throughout the consumer data journey (which, by and large for marketing purposes, will be based on either consent or legitimate interest), then the kinds of third party data offered by reputable marketing services organisations can play a vital role in the marketing activities of many brands and organisations.

Businesses must have ensured that they have communicated to their customers that this type of processing will take place and the organisations it will be shared with in their privacy policies – and that they have their own legal grounds for processing.

They should also recognise that when using third party data there may be no direct relationship with the data subject which should be given due consideration in terms of assessing potential risk. Such risks can be mitigated through contractual controls and robust supplier due diligence. Article 14 of the GDPR deals specifically with the need to inform data subjects about how their data will be used if it was not collected directly from them.

References and further reading

DMA Guidance on Consent and legitimate interests

https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

ICO Guidance on Consent

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO Guidance on Legitimate Interests

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Right to be informed

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

What marketing benefits does using third party data bring to organisations?

Organisations could choose not to use third party data. But this is to ignore the significant opportunities that compliant, robust and high quality third party data offers brands and organisations prepared to deploy it correctly and compliantly.

There are huge advantages for brands and organisations in providing support, insight and market context to grow their customer base, to develop appropriate products and services for their marketplace and to provide relevant and appropriate marketing experiences to existing and potential customers.

Brands still need to ensure that the activities that are conducted are justifiable under GDPR and PECR, but the benefits for third party include

- Combing first and third for higher returns

  The inherent power of first party data doesn't mean that the role of third-party data is redundant. In fact, organisations that report the highest return on their data-related investments are more likely when first-party data gets enriched by third-party data.

- Adding context

  Third-party data, like some of the consumer marketing data and segmentation that marketing services organisations provide, adds context to an organisation's customer base and enables demographic, location, behavioural and contextual targeting.

- Creating breadth and depth of insight

  It enhances the breadth and depth of insight which would be hard to derive from a single data source (such as you're a brand's first-party data) and has implications for product / service development in ensuring that the organisation is developing the right things for the marketing they are serving – ultimately benefiting the consumer.

- New audiences at scale

  For customer acquisition, it is key when trying to reach an audience at scale that you don't have first-hand information about. Likewise, it enables you to gain greater insight on individuals to avoid sending them inappropriate offers in relation to their likely circumstances (and this applies both for new customer acquisition and existing customers).

- Understanding digital behaviour

  In the digital programmatic advertising world, advertisers use third party data every day to increase campaign efficiency by identifying desired audiences and allotting ad spend accordingly. Through linkage between offline and online data, it is used to target audiences with ads or to serve bespoke messaging to certain segments.

  It can indicate a user's digital actions, inferred interest or location behaviour so that organisations can provide their customers with more relevant marketing experiences across all channels.

- Helping small organisations grow

  For smaller organisations who have very little customer data, or for organisations that don't collect first party data at all, the ability to use third party data is vital to grow their businesses and to market to consumers who are likely to respond positively to their offers. In these organisations, third party data helps to fuel innovation through business growth and has an economic impact which is important at a national level.

Why third party data benefits the consumer and the economy

We're all consumers.

When we choose to engage with brands, the use of third party data by organisations ensures that the offers and services marketed to us by brands are more likely to be relevant and personalised, enabling brands to communicate with us at the right time, through the right channel andon the right device.

In a busy world all of this saves us time because we are served marketing communications based on our observed or likely interests.

When used as part of a responsible marketing campaign by ethical brands who respect their customers' wishes, the use of third party data enables organisations to deliver great customer services and build trust in the way personal data is being used.

Lawful and appropriate use of third party data not only benefits individual companies and consumers, but it also produces broader societal benefits by increasing choice for consumers and fostering fair competition among businesses.

In the retail sector for example, third party data is often used by SMEs that do not have large distribution networks to reach consumers directly and challenge more established retailers. This not only allows new brands and products to come to market providing more choice for consumers, but also boosts competition across existing businesses. Competition in turn helps to reduce prices and improve product quality, as recognised by the European Commission.

The consideration of the benefits that the lawful and appropriate use of third party data generates for society is clearly expressed in Recital 4 of the GDPR (reported below for reference):

"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

This is also referenced in the "Lawful basis for processing: Legitimate interest" guidance by the ICO (see page 10, "What's new under the GDPR?"):

"Legitimate interests that are relevant are no longer limited to your own interests or those of third parties to whom you disclose the data. You can now consider the interests of any third party, including the wider benefits to society".

Linkage: What is it and what can it be used for?

Customer names and addresses, emails and digital identifiers may be matched with third party identity data to consistently identify an individual, household, location or device.

This brings together fragmented data into a coherent, consistent view of a client's known customers and to connect and link this first party data to other marketing and advertising databases, platforms and channels.

As well as current identities, this third-party data may also include historic and alternative identities, for example "movers" data to indicate where a consumer has moved address, aliases, alternate contact details / emails.

This is referred to as "linkage" and is the "bridge" between online and offline environments to support advertisers that wish to push and pull compliantly held first party data on their consumers, into an online environment

Often held against this third-party identity data is demographic, attribute, segmentation and modelled data, enabling additional insight about a business' known customers to be applied to any linked data for marketing purposes.

Links may also be provided to first party data entities such as data controllers and processors to assist them in recognising and resolving a single customer view, cleansing and validating first party and partner data.

The 'Linkage' application of third party data under GDPR may be undertaken using legitimate interest (LI) as data is only ever used to resolve identity, validate details or link a known individual's details across platforms. This is often done to comply with the requirements of keeping data up to date.

To ensure GDPR standards of transparency, notice and choice, third party data providers must ensure that notice of LI is provided via third party data Partner Source Notifications.

Additionally, first party data Client Privacy Notices must meet the relevant transparency requirements, with an obvious and accessible opt-out of legitimate interest processing activity.

The ICO and industry guidance recommends that Legitimate Interest Assessments (LIAs) must be undertaken if organisations are seeking to rely on the Legitimate Interest ground.

For example:

- Targeted online advertising

  A brand that holds names and addresses and email addresses of its customers might wish to link these to digital identifiers (cookies, devices etc.) by using a third party that has created a GDPR compliant and permissioned 'pool' of these identifiers with associated email addresses and/or postal addresses.

  Once the link has been made, the brand now has a cookie associated with its customer name and address data. This allows the brand to use the digital advertising ecosystem and programmatic media buying to target personalised advertisements across a range of web sites. This advertising itself will typically be carried out on behalf of the brand by its media agency.

  Legal basis: Consent under PECR e.g. the individual has consented to having cookies dropped on their device.

  However, any processing of personal data to support the serving of the advertising (e.g. using linkage to help create a relevant audience) may be done under legitimate interest.

- Targeting an unknown cookie or device online using a broad segmentation

Digital marketing can leverage offline third party data through the appending of this data onto a cookie or device.

If there are user registration details available, this might be enabled through linking a user's postcode to, say, a third party geodemographic segmentation or audience segment.

More likely, this linkage might be based on a geographic match based on an IP address or on location data (XY coordinates) linked to a device. Some providers can further refine this by identifying likely home location or postcode.

Legal Basis: For data providers the legal basis could be legitimate interest to enable the linkage and to build / create the digital audience. Geolocation data may be seen as particularly privacy-intrusive, so additional care needs to be taken with the LIA.

But an advertiser needs to ensure that the cookie/device has been captured with the appropriate notification/consent and that any data manipulation by the DMP/AdTech provider is appropriate and done with the right legal grounds for processin

- Tagging a customer file with targeting variables

A brand wishes to acquire additional information about its customers. Third-party data companies hold data about UK consumers derived from many sources, including the edited Electoral Roll, market research surveys, information collected directly from consumers via lifestyle questionnaire, etc.

This data will include real and modelled data variables and segmentation solutions at address, household and individual level. The name and address held on the third-party database may be matched to the customer name and address on the brand's database.

Once linked, any of the targeting variables on the third-party database may be transferred or "tagged" to the customer name and address and then used for a range of marketing purposes (see Analytics and Contact Use cases).

Legal basis: Depending on the context of the variables, this may be done under legitimate interest

- Single customer view

A brand may hold data on its customers but in different databases in various parts of the business.

At the same time, a consumer could have several ways that they identify themselves, current or historic or interact with the brand – and this can include name at an old address, several email addresses, aliases or a name with just a digital identity.

As a result, the brand or organisation does not have a full and consistent view of its relationship with that customer. Third-party data quality services and linkage data may join all of these customer identities together to produce a single customer view of the brand's relationship with that person.

This means the brand can communicate much more effectively with the customer and provide a consistent and relevant customer experience across channels, drawing on the full range of information held about that customer and their channel preferences.

A good example here would be making sure a retailer who has physical stores, a website, an app and a social media presence, provides you with a consistent experience and set of offers across all these contact points.

Legal basis: Legitimate interest

- Identity management

  The name and address on a customer file may be linked to various third-party databases either to check that the information they hold about that person is accurate and up-to-date or to check something else about the person.

  This would include matching to various suppression files, such as the Mailing Preference Service (MPS) or Telephone Preference Service (TPS) and various bereavement registers, as well as to validate current address details or credit status.

  This use of linkage allows the brand to ensure it has accurate information when communicating with its customers, which is a key GDPR principle.

  Legal basis: Legitimate interest

References and further reading

DMA Guidance on Consent and legitimate interests

https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

ICO Guidance on Consent

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO Guidance on Legitimate Interests

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Right to be informed

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=62227

Analytics: What is it and how is it used?

Third party data is widely used by organisations for analytics and insight purposes. A useful source of information on this is the ICO's Big Data, AI, and Machine Learning paper.

This data can be personal data, anonymised or pseudonymised individual level data and aggregated data (often relating to geographical areas). It is good practise to anonymise any personal data if there is no requirement to know who the individual is when undertaking any analytics, so data is not personally identifiable during the analytics work.

Where personal data is involved, most analytics and insight use cases may be undertaken based on legitimate interest, although the business will need to ensure it is transparent for the consumer to know what is happening with their data.

Please remember if the purpose of the analytics is to identify relevant audiences for a marketing communication, appropriate permission must exist to send this communication (and this will depend on the communication channel).

For example:

- Data enhancement and insight

  A brand may obtain targeting variables about its customers from a third-party data supplier (see use case three in Linkage above).

  This data enhances the information the brand already holds about that customer and enriches it. The third-party data can be used in various analytical projects. These might include creating a segmentation of the customer base, allowing different creative designs and contact strategies for different types of customer.

  The data may also be used, perhaps in combination with data already held about the customer, to create modelled scores that aim to predict likely future needs or behaviour of the customer.

  This might include the propensity to purchase additional products and services or likelihood to defect to a competitor brand.

  The data appended (models derived from this) may be applied across a client's CRM, call centre, web analytics, DMP and any other environment with full or partial first party data for the purpose of marketing or customer service.

  Legal basis: Legitimate interest

- Strategic decision making

  Third party data can be useful for organisations who are planning their future strategy – in terms of the markets that they want to compete, audience selection and the products and services that they should develop and offer.

  Relying on their own first party data only provides a window on the market opportunity but supplemented with third party data a more complete view of the UK landscape is available with which to plan a robust market strategy.

  Location planning examples would include setting branch managers targets or helping decide on where to site new stores based on the characteristics of the people that live in the neighbourhood.

  Legal basis: Legitimate interest

- Attribution and measurement

  Third party data about the outcome of a marketing communication e.g. impressions viewed, emails opened, other websites viewed in a session enables analytics teams to measure the impact of their organisations marketing activities and to attribute the campaign spend to appropriate channels to get a better view of marketing efficiency.

  This kind of analytics use of third party data is particularly important in digital channels. Legal basis: Legitimate interest

- Conducting research and surveys

  When conducting market research surveys, third party data is often used by analytics teams to produce a sampling frame to ensure the survey is completed by a representative group of individuals e.g. representative of the demographic distribution of the UK population.

  When survey research is completed, third party data could be appended to the respondent details to that in aggregate analysts can use the survey results to look at behaviours across third party segments or other data.

  Legal basis: Legitimate interest

References and further reading

DMA Guidance on Consent and legitimate interests

https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

ICO Guidance on Consent

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO Guidance on Legitimate Interests

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Right to be informed

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Contact: What is it and what is it used for?

Use of third party data for contact is where an organisation obtains contact details of a consumer for marketing purposes from a third party, as opposed to collecting it direct from the consumer.

Contact details might include name and address for direct mail campaigns, telephone numbers for telemarketing or digital identifiers such as email address or digital identifiers for digital campaigns.

The aim of obtaining this data is for the organisation to communicate directly with the consumer, usually to inform them about the products and services the organisation has to offer in order to find new customers (customer acquisition).

In most cases where appropriately permissioned third party contact data is provided to organisations for contact purposes, additional third party information such as modelled propensities or segmentation codes may have been used to ensure that this contact "audience" contains individuals to which the marketing offer is likely to be appropriate.

For example:

- Customer acquisition

  All brands need to acquire new customers. Prospect data is available from many third party data sources. Lists of names and addresses can be purchased for direct mail campaigns. The names may be sourced from the edited Electoral Roll or other compliant sources and selected using targeting criteria held against the names and addresses on the third-party database or a file of customer name and addresses may be matched to the third-party database and "lookalikes" chosen for a prospect mailing. Other third-party prospect data will have been collected directly from consumers, where they will have expressed an interest in receiving offers from relevant brands.

  Telephone numbers and email addresses can also be purchased for telemarketing and digital marketing campaigns in a similar manner, although the DMA recommends that for email prospect acquisition by email, this is done through an affinity marketing campaign / host mailing where the emails are broadcast by the originator of the personal data.

  Legal basis: Whilst consent is an option, legitimate interest is the preferred grounds for postal direct mail.

  Publicly available name and address data such as the Edited Electoral Register (EER) may be used for contact purposes under legitimate interest. If people wish to opt out of unsolicited communication by direct mail, they can register with the MPS to register their objection. Article 14 of the GDPR deals specifically with the need to inform data subjects about how their data will be used if it was not collected directly from them. This should be done on first contact with the consumer.

  Legitimate interest cannot be used for contact purposes for electronic communications, where consent is needed to be compliant with PECR.

- Email and reverse email append

  There are third-party databases that will allow a brand to match a name and address to a database where that name and address also occurs but had an email address associated with it.

  If the brand does not have an email address for that person, it gives the brand the opportunity to communicate with them through an additional channel, although PECR regulation is important here: Any initial marketing contact by email with an individual must be undertaken by the organisation that holds the consent to contact that individual by email (this is often initiated through a host emailing service where the

originator of the consent introduces the brand by email to the consumer).

The same process may be carried out in reverse.

If a brand has an email address, this may be matched into a third-party database and a connected name and postal address can be provided back to the brand.

Legal basis: Consent required to contact a prospect through email; consent or legitimate interest for any postal communication.

- Digital marketing and social media advertising

In the same way that a brand can obtain names and addresses from a third party for a direct mail campaign, it may use third party data to create a relevant audience that matches the brand's criteria for the digital marketing campaign (for example, an audience made up of certain segment types or from models which indicate a high likelihood of exhibiting certain behaviours).

Such a campaign could be executed through a digital publisher such as a media website or a social media platform.

This audience can be made up of a subset of existing customers, selected using third-party data, where the brand may upload a file of these customers to the publisher or social media platform.

Where the same people are registered users of the site or platform and have agreed to receive ads, serve them an ad to cross-sell or up-sell the brand's products. Alternatively, this might be a prospect audience created by the third party and which is then, through linkage, matched into the user base of the publisher or social media platform.

Providing the prospect is a registered user of the publisher or platform and has given them the relevant permission to display ads to them, the campaign can be served to that audience through the platform.

Legal basis: In this context, third party data is mainly used to create a relevant audience to inform relevant advertising through publisher websites, apps, social media and other digital channels such as addressable TV advertising.

The processing activities (e.g. building an audience) to enable/support this advertising may be done under LI but the serving of the digital communication by the publisher or the social media platform will need to be based on permissions that they has with their users, either through cookie-based consent or user permissions settings in a social media platform (as PECR is relevant here).

- Digital customer acquisition

Brands looking to acquire new customers in the digital ecosystem can use the same appropriately permissioned data from the sources named in customer acquisition below the line marketing.

Name, address, and email selections or look-a-likes of prospects from these compliant data sources and then linked (see above) into a digital platform (e.g. DMP or DSP) for media buying or website personalisation.

Legal basis: Whilst consent is an option, legitimate interest is the recommended grounds for this type of marketing.

The processing activities (e.g. building an audience) to enable/support this advertising may be done under LI but the serving of the digital communication by the publisher (or site personalisation) will need to be based on permissions that the publisher/business has with its users (as PECR is relevant here).

- Targeted online "behavioural" advertising

  A brand wishes to advertise a particular product or service online.

  It can use cookies from a third-party database that have various attributes associated with them, based on browsing behaviour.

  This allows them to create an amplified digital audience that meets that brand's targeting criteria – and permits the brand's media agency to use the cookies for an online advertising campaign.

  Legal basis: Again, third party data is mainly used to create relevant audiences to inform relevant advertising.

  The processing activities (e.g. building an audience) to enable/support this advertising may be done under LI but the serving of the digital communication by the publisher will need to be based on permissions that the publisher has with its users (as PECR is relevant here).

The GDPR has elevated both the regulatory and ethical due diligence required to be conducted across the marketing industry relating to third-party data use.

Across all use cases of third party data it is important that the brand or organisation using the third-party data reassures themselves that data is compliant by conducting appropriate due diligence on the source of that data.

Brands and organisations also have a responsibility to ensure that the uses to which they intend to put this data are transparent to consumers, and that regulatory and ethical considerations are made on the use of this data.

The DMA will produce separate guidance on best practice due diligence responsibilities of first party data taking into consideration third party data and the due diligence that third party data providers need to undertake on their data sources.

If the provided third party data is sourced and processed by the data providers compliantly - and used compliantly and responsibly by brands and organisations - then this should increase trust and reassurance in the use of this data, by both organisations and consumers.

In this context, third party data will continue to play a significant role in providing support, insight and market context to brands and organisations to grow their customer base, to develop appropriate products and services for their marketplace and to provide relevant and appropriate marketing experiences to existing and potential customers.

References and further reading

DMA Guidance on Consent and legitimate interests

https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

ICO Guidance on Consent

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO Guidance on Legitimate Interests

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Right to be informed

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

About the DMA

A DMA membership will grow your business.

Our network of more than 1,000 UK companies access research, free legal advice, political lobbying and industry guidance. DMA members connect at regular events that inspire creativity; showcase innovation; examine and provide insights from award-winning campaign work; and grow our understanding of how responsible marketing and the GDPR will transform how we all work.

Membership of the DMA acts as a badge of accreditation and we provide expert-led guidance across channels, underpinned by a code that puts the customer at the heart of everything we do.

We represent a data-driven industry that leads in creativity and innovation: a sector that attracts the brightest minds, the individuals that will shape the future.

By sharing our knowledge, together, we'll make it vibrant.

Find out what we can do for you: membership@dma.org.uk