



# DMA advice: GDPR - a training guide for contact centre agents

June 2018

Published by The Contact Centres Council



# Contents

|   |    |
|---|----|
| Acknowledgements .....  | 2  |
| Introduction .....  | 3  |
| Who is this guide for? .....                                      | 4  |
| What has changed? .....   | 5  |
| Area .....  | 5  |
| Data Protection Act 1998 .....                                    | 5  |
| New Data Protection Act (GDPR) .....                              | 5  |
| Who should design the training? .....                             | 9  |
| When to deliver the training? .....                               | 9  |
| Should the data protection training be scored? .....              | 9  |
| How can we ensure knowledge is maintained? .....                  | 10 |
| Should I change my quality monitoring criteria / scorecard? ..... | 11 |
| Training design ideas .....                                       | 12 |
| How long will you be keeping my data for? .....                   | 13 |
| How long will you be keeping my call recordings for? .....        | 14 |
| Where did you get my data? .....                                  | 15 |
| What do you plan to do with my data? .....                        | 16 |
| Why are you capturing my email address? .....                     | 17 |
| Why do you need to know my age? .....                             | 18 |
| Do you profile my data? .....                                     | 19 |
| How do I know when someone is opting out? .....                   | 20 |
| Permissions / consent .....                                       | 21 |
| Consent gaining training .....                                    | 21 |
| Summary .....   | 22 |
| About the Contact Centre Council .....                            | 23 |
| About the DMA .....   | 24 |



# Acknowledgements

The DMA wishes to thank the following members for their contribution to these guidelines:

**Nerys Corfield** – Injection Consulting

**Lisa Chambers** – KMB

**Dave Clark** – NTT Fundraising

**Martyn Daly** – Dignity UK

**David Freedman** – Confero

**Ben Lappin** – The Guardian

**Christopher Stransom** – Age UK

**Steve Sullian** – Channel Doctors

**Alistair White** – Noetica



# Introduction

GDPR (EU General Data Protection Regulation) came into force on 25 May, this and the 2018 UK Data Protection Act (2018 DPA) changes the way customers engage with brands.

Trust will become a more vital component of the relationship and this trust will be gained through transparency.

Empowering your front-line agents to have a fully rounded view of your data policies is really important.

The Contact Centre Council has produced the below guide to help provide a practical guide on the areas your Contact Centre training will need to change.



# Who is this guide for?

This guide is for anyone involved in training front-line agents.

Considering the rich variation of contact centres who will be referencing this guide it is impossible to be prescriptive.

With this in mind the guide is a collection of key areas for consideration when ensuring agents feel confident to respond to queries that are more likely to be raised as a consequence of the ever-increasing focus from consumers on the protection of their data.

Why do I need to change the training?

Your current training will need to be overhauled or adapted to cover the impacts of the GDPR / the new Data Protection Act.

It is anticipated that there will be a consumer facing campaign to inform the public about their rights in respect to their personal data.

This knowledge could mean more questions, and - more importantly - more informed questions, are posed to the front-line teams.

The GDPR also includes a new Accountability principle, which means that organisations must clearly demonstrate that they comply with the new data protection requirements.

As a responsible employer you should re-train/re-brief all existing staff, deliver a new data protection section for new starters and have a documented process for ensuring your employees' understanding is maintained. It's always worth remembering:

***"Of the 99 articles in the GDPR, more than half are tied to requirements that, if infringed, can lead to fines in the millions."***

Source: [DPNetwork.org.uk](http://DPNetwork.org.uk)

In a recent DMA study in respect to data it was found that trust was cited in the top three considerations for data exchange by over 50% of consumers surveyed and 88% of consumers stated transparency over data collection is key when collecting personal data.

Consumers' trust in the way you treat their data will become a greater factor in your relationship, thus offering opportunities to increase trust and loyalty, or present increased risks of breaking trust and loyalty.

# What has changed?

This table provides a top line view of the key areas of the new Data Protection Act.

| Area                        | Data Protection Act 1998  | New Data Protection Act (GDPR)   |
|-----------------------------|---|--|
| Definition of Personal Data | "personal data" - any data that can be used to identify a living individual: name and address, telephone number or email address.   | Now includes on-line identifiers i.e. location data; an online name; IP addresses and mobile device IDs.   |
| Consent                     | "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".  | If processing data on the basis of Consent (and not Legitimate Interest) it needs to be unambiguous; Requires a positive opt-in; Be specific and granular (channel); Keep evidence of Consent – Who, When, How and What you told people.   |
| Privacy Statement           | <p>information available to the data subjects (the individuals whom the data relates to), so far as practicable: who the data controller is; the purpose or purposes for which the information will be processed; any further information which is necessary in the specific circumstances to enable the processing to be fair.</p> <p>This applies whether the personal data was obtained directly from the data subjects or from other sources.</p> | <p>The privacy notice is a key component in outlining exactly who will be using data, the context in which it will be used, thus informing and further shaping the data subject's realistic expectations.</p> <p>There is a fundamental obligation to tell data subjects what their personal data will be used for and the privacy notice is where a business must showcase and record such activities.</p> <p>The GDPR includes a longer and more detailed list of information that must be provided in a privacy notice than the DPA does. from data subjects or from a third party:</p> <p>There are also some differences in what you are required to provide, depending on whether you are collecting the information directly from data subjects or from a third party:</p> <p>Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer</p> |

|                          |  |   |
|--------------------------|--|---|
|                          |  | <p>Purpose of the processing and the legal basis for the processing</p> <p>The legitimate interests of the controller or third party, where applicable</p> <p>Any recipient or categories of recipients of the personal data</p> <p>Details of transfers to third country and safeguards</p> <p>Retention period or criteria used to determine the retention period</p> <p>The existence of each of data subject's rights</p> <p>The right to withdraw consent at any time, where relevant</p> <p>The right to lodge a complaint with a supervisory authority</p> <p>The source the personal data originates from and whether it came from publicly accessible sources.</p> |
| Children                 | Not part of the 1998 Data Protection Act | In the UK only children aged 13 or over can give consent for the processing of their personal data in relation to information services.   |
| Rights to Portability    | Not part of the 1998 data protection act | The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.   |
| Data Protection Officers | Not part of the 1998 data protection act | <p>Under the GDPR, you must appoint a DPO if you:</p> <p>are a public authority (except for courts acting in their judicial capacity);</p> <p>carry out large scale systematic monitoring of individuals (for example, online behavior tracking);</p>   |

|                      |   |   |
|----------------------|---|---|
|                      |   | <p>or carry out large scale processing of special categories of data or data relating to criminal convictions and offences.</p> <p>You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.</p> <p>Any organisation is able to appoint a DPO.</p> <p>Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.</p>  |
| <p>Data Breaches</p> | <p>There is no legal obligation on data controllers to report breaches of security.</p> | <p>Under the GDPR, a “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”</p> <p>Data controllers and data processors are now subject to a general personal data breach notification regime</p> <ul style="list-style-type: none"> <li>• Data processors must report personal data breaches to data controllers</li> <li>• Data controllers must report personal data breaches to their supervisory authority and in some cases, affected data subjects, in each case following specific GDPR provisions</li> </ul> <p>Non-compliance can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.</p> |



|                                |   |   |
|--------------------------------|---|---|
| Fines                          | Maximum of £500,000   | Maximum £17 million or 4% of global turnover allowed under the new law.   |
| Profiling                      | <p>This used to be under 'Automated decision making'. Subject access allows an individual access to information about the reasoning behind any decisions taken by automated means. The Act complements this provision by including rights that relate to automated decision taking.</p> <p>Consequently:</p> <p>an individual can give written notice requiring you not to take any automated decisions using their personal data;<br/> even if they have not given notice, an individual should be informed when such a decision has been taken; and<br/> an individual can ask you to reconsider a decision taken by automated means.</p> | Any form of automated processing of personal data used to analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, etc.  |
| Subject Access Requests (SARs) | <p>The individual has a right to request access to the information a controller or processor has on you.</p> <p>Organisations may charge a fee of up to £10 (£2 if it is a request to a credit reference agency for information about your financial standing only).</p> <p>There are special rules that apply to fees for paper based health records (the maximum fee is currently £50) and education records (a sliding scale from £1 to £50 depending on the number of pages provided).</p>  | <p>The GDPR re-states individuals' right to request confirmation that their personal data is being processed.</p> <p>Access to that personal data<br/> But in future organisations will have to provide the data free of charge and in most cases do so within a month.</p> |

# Who should design the training?

If you do have a Data Protection Officer\* it would be prudent for them to work in conjunction with the training team.

It would also be a good idea to include the Marketing, IT and CRM team in the design of the training.

Essentially, you should engage with as broad a group of stakeholders as possible, but ensure that the final training is designed by your colleagues who understand the environment and challenges faced by your front-line agents.

If you:

- Are a public authority
- Carry out large-scale, regular and systematic monitoring of individuals, or
- Carry out large scale processing of 'special categories' of data

Then you will have appointed a Data Protection Officer – but you may decide to appoint one even if your organisation doesn't fulfil these mandatory criteria.

## When to deliver the training?

All new starters are trained as part of their induction and that a re-brief/re-training programme is conducted annually.

We recommend all operational staff – not just those directly interacting with customers -are trained on the new regulation.

## Should the data protection training be scored?

Yes training should be scored.

It would be prudent to create a test which the staff either pass or fail, as a way of establishing knowledge and understanding levels post-training.

Our recommendation is to update your proof of learning policy to include a percentage of data protection questions (to include the new regulations) and carry out a test similar to that undertaken for the theory section of a driving test i.e.

Are we processing data on the legal basis of:

- Legitimate interest
- Consent
- Vital Interest

***NB – all of the above could be correct***

## If someone is asking you to send them all information we hold on them should you...

- Tell them that is not possible
- Give them the email address/telephone number of the team who process these requests
- Ask questions to determine what specific information the data subject is interested in and why they are interested in it

***NB – both b and c could be correct dependent on your internal processes***

**Should agents who fail the data protection component of training be delayed from taking/making calls?**

Yes, staff should not be allowed to process personal data until they have demonstrated an understanding of the regulatory requirements as they impact on their roles.\*

**How can we ensure knowledge is maintained?**

To ensure this knowledge is maintained you might want to consider:

- Running annual refresher training
- Carrying out mystery shopping
- Making sure your QM scorecard has Data Protection adherence as a separate section.
- Using down-time to present agents with quick fire questions
- Running data protection road-shows
- Including a score in your employee engagement surveys specific to confidence levels around the data protection act

Any staff demonstrating a lack of understanding should be removed from active duty and appropriately supported and coached until they have demonstrated the required competence.\*

The results of all tests should be kept and stored in peoples personal records and be fully auditable if required.\*

The person responsible for maintaining and validating organisational and employees' data protection knowledge should be made clear in a governance model.

If agents have questions or gaps in their understanding then the points of escalation and clarification should be made clear to them.

These internal data protection specialists should be given the opportunity to develop a strong understanding of the requirements and their context for your specific organisation.

**\*remember that any additional requirements on employees will need to be reflected in their employment or service contracts**



# Should I change my quality monitoring criteria / scorecard?

The presenting of permission statements, the requesting of personal data and the responding to questions centered around data protection and data subjects' enhanced rights will all be important elements to train and coach agents on.

Agents' knowledge and understanding, as well as the soft skills to confidently and assuredly share their understanding with consumers should both be assessed and scored.

In line with the Accountability Principle you should probably look to include data protection in both the knowledge and skills sections of any generic framework and scorecards.

The relative importance and weighting will need to be agreed internally.



# Training design ideas

The below gives suggestions on what you could present to your agents - the level of insight you choose to provide will be dependent on your internal factors:

- Take all data capture fields and provide an overview of why each data capture field is used
- Give them an understanding of the consequences of not adhering to the new guidelines for both the organisation and the individual employee (dependent on your organisation's disciplinary and performance management approach)
- Revised permission statements (or use of alternative bases for processing, such as Legitimate Interest)
- Overview of data owner and processor
- Call recording retention policies
- Subject Access Request Customer Journey
- Right to Erasure Request Customer Journey
- Social Media data capture and data governance processes
- FAQs

The below section gives some anticipated common FAQs.

These should be covered in training; should also be accessible in a knowledge base, audited regularly and up-dated in line with any data changes (ensure you have allocated an owner to keep this document up-dated).

# How long will you be keeping my data for?

The regulation states that data should be “kept in a form which permits identification of data subjects for no longer than necessary” [GDPR Article 5, clause 1(e)].

In other words, personal data that’s no longer justifiably required should be deleted.

## Training Guidance

Processor – confirm with your data controller but keep it a generic ‘standard process’

Controller – tell the agents to look at the data privacy statement

The [ICO](#) guidance in respect to the retention of personal data will need to be referenced

### [Data Retention from the ICO](#)

The agents might need to know how long data records will be kept for, why data is being held and what happens to the data at the end of the retention period.

It would also be good to give them the understanding of how the security of this data is maintained.

There is no specific guidance on this point - it is up to organisations to determine.

Data may be retained for different retention periods for different purposes. The Accountability principle is also relevant here.

The customer must have been informed of the retention period or how the retention period is calculated in accordance with the information requirements under Article 13 and 14 of the GDPR when their personal data was first calculated.

NB. Organisations in specific business sectors will have rules that apply to them (e.g. Financial Conduct Authority rules for companies in financial services), which may require that data is retained for different specific periods

# How long will you be keeping my call recordings for?

The regulation states that data should be “kept in a form which permits identification of data subjects for no longer than necessary” [GDPR Article 5, clause 1(e)].

In other words, personal data that’s no longer justifiably required should be deleted.

## Training Guidance

### [Data Retention from the ICO](#)

The agents need to know how long call recordings will be kept for, why call recordings are being held and what happens to the call recordings at the end of the retention period.

It would also be good to give them the understanding of how the security of these call recordings is maintained.

Provision should be made during the training to the legalities around the retention of call recording as two separate entities, that of the customer at the point of obtaining data, what data is captured and how that data will be stored and processed further according to Article 13 and 14 of the GDPR in respect of personal information held about them.

In addition the agent will also need to be advised about the retention of calls that they have made and how this data will be processed and stored and retained as required by Article 13 and 14 of the GDPR in respect of how this personal information is held, examples of how their calls are used for quality assurance, who would have access to these calls and scoring applied to them for performance purposes could be used.

The retention periods for call recordings both from the personal data about the agent and the personal data of the customer need to be separated out.

The agent and the customer both need to be given separate information notices as required by Article 13 and 14 of the GDPR in respect of personal information held about them on the 25 May 2018 and new staff members and customers who join after 25 May 2018 need to be given this information when their personal data is first collected

NB. Organisations in specific business sectors will have rules that apply to them (e.g. Financial Conduct Authority rules for companies in financial services), which may require that call recording data is retained for different specific periods



# Where did you get my data?

## **Training Guidance**

The answer to this question will vary greatly from organisation to organisation and even between prospect or customer groups within an organisation. In order to be able to answer this question your front-line teams will need:

Inbound:

Consent and Privacy Policies to be compliant and comprehensive (as a must). A view on permissions provided including the date given (access to a permission centre).

Outbound:

Access to a data management solution that can provide a granular view of the point of origination of a prospect or customer record.

Consideration needs to be given to the possibility of the legitimate interest legal ground being used and to the information notice requirements under Article 13 and 14 of GDPR

NB: Employees have a right to know what data you hold on them.





# What do you plan to do with my data?

The regulation states that you must explain what you will do with people's personal data and why at the time at which they share it with you. Your privacy or information notice should include your lawful basis for processing as well as the purposes of the processing.\*

\*Source - ICO: Guide to the General Data Protection Regulation (GDPR), 21 November 2017

## Training Guidance


The ICO supports the notion of 'layering', by which a privacy notice (which has to be both comprehensive and detailed, as well as easily understood) can be broken down into 'layers'.

So there's a comprehensive but high-level description of what you will do with your customers' data, followed by more detailed descriptions that – online – a customer could click to read.

This can be adapted for phone calls so that an agent can offer subsequent levels of detail if the customer would like to hear it.

Make sure this section of the training is very clear and transparent, but that doesn't mean that it can't be covered in a very positive way.

Show the customer data journey and highlight the benefits this will mean to the caller – e.g. a more personalised communication delivered at the most appropriate time (with the most relevant offer / information).



# Why are you capturing my email address?

The regulation states that you must explain what you will do with people's personal data and why at the time at which they share it with you. Your privacy or information notice should include your lawful basis for processing as well as the purposes of the processing.

## Training Guidance

Make sure this part is very clear and is covered in a positive way.

The capture of email on a voice call demonstrates a real commitment from the consumer to engage with the brand so priming the agents to ask on every call, make sure they are clear on what the email customer journey will look like and that they have access to the privacy policy will all be crucial in gaining email data capture.

Examples of positive messages:

We are keen to be able to communicate with our customers in the way that best suit them. Most customers find that email is a convenient way of receiving non-urgent information (You should have the ability to record customers' channel preferences – including their preferences by type of contact)

We use your email address as a customer identifier, to help us know that it's you who's making contact with us – either in-person or via our self-service portal – and allowing us to be sure that we are protecting your personal information

We want to deliver messages that are relevant to you and your needs at a time that is most convenient to you

# Why do you need to know my age?

The regulation states that you must explain what you will do with people's personal data and why at the time at which they share it with you. Your privacy or information notice should include your lawful basis for processing as well as the purposes of the processing.\*

\*Source - ICO: Guide to the General Data Protection Regulation (GDPR), 21 November 2017

## Training Guidance

A key principle of the GDPR / 2018 DPA is to avoid retaining any personal data if you don't have a compelling need for it.

Unless there is a justifiable reason for capturing someone's age i.e. it's important because you are selling a product or service that's restricted to a certain age group (e.g. adults-only, for children, for aged 60 plus, etc.), or for which pricing or service levels are age-dependent (e.g. some insurance products) then its justifiable and can be explained to the agents.

If the reason is not clear then this needs a wider review before proceeding down this route as it's not an easy question for agents to ask and without a justifiable reason for capturing it consumers could be wary and the GDPR / 2018 DPA principles will be compromised.

# Do you profile my data?

## Training Guidance

If you are a company that profiles data then we advise you to get some advice from your DPO on what affect this will have on the consumer and advise your agents appropriately.

Consumers have the right to withdraw from automated profiling and profiling for marketing purposes, in which case the process of removing a consumer from the profiling should be explained simply and clearly to your agent to pass on to the consumer if asked.

### I want to check the data you have on me – how do I go about this?

The regulation states that, under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).\*

\*Source - ICO: Guide to the General Data Protection Regulation (GDPR), 21 November 2017

## Training Guidance

Your internal process and what the consumer can expect needs to be clearly outlined to agents. Are you going to allow SAR's to take place over the phone? Will all of your agent community be able to manage SAR's or will you have a specialist team trained that they will need to transfer to/provide an email address for?

Before a SAR is processed make sure the agents are clear on what they need to do to assure them of the customer's identity. It is worth including IT in the conversations when designing the training in this section.

For most organisations the best way to provide customers with clarity and control over their personal data is by developing a privacy centre or portal: these provide customers with a self-service route to manage their data and preferences.

I want to be forgotten / I want to be erased from your database – what do I need to do and when is this going to happen?

The regulation states that the right to erasure is also known as 'the right to be forgotten'.

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.\*

\*Source - ICO: Guide to the General Data Protection Regulation (GDPR), 21 November 2017

# How do I know when someone is opting out?

The regulation states that the GDPR / 2018 DPA gives a specific right to withdraw consent. You need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time.

\*Source - ICO: Guide to the General Data Protection Regulation (GDPR), 21 November 2017

## Training Guidance

Similarly to the Right to Erasure, you need your front line teams to understand exactly what it is that the customer wants to 'opt out' from?

Do they object to marketing communications, or just those via some channels? Or perhaps for some products and not others.

The better the data management technology available to your customers and front-line staff, the better individual preferences can be respected and reflected

## What to do if your agent does not know the answer to these questions?

Make sure there is a clear escalation route.

# Permissions / consent

## Permissions / consent

With a requirement to hold information in the database of who, how and when consent was gained, it would be prudent to present this information to advisors on their desktop (for both inbound and outbound) when a call is presented so they can respond appropriately if challenged.

If as a business you are using consent as the basis for processing personal data (there are six lawful grounds for collecting personal data) then will have created your consent statements and your customer journey to determine how and when over a lifetime of a customer permission will be gained and when re-permissions will take place.

Training your agents to gain permission in a 'clear and concise' way that remains in line with the tone and flow of the conversation will become very important.

"Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.

Getting this right should be seen as essential to good customer service: it will put people at the centre of the relationship and can help build customer confidence and trust.

This can enhance your reputation, improve levels of engagement and encourage use of new services and products. It's one way to set yourself apart from the competition".

Source: ICO

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid: in particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent.

It is worth remembering that ICO guidance states that gaining consent shouldn't disrupt the customer experience. If your consent is going to be layered in a user-friendly way (i.e. giving the customer the option to hear details specific to your third-party processors) then make sure these layers are outlined clearly in the training.

## Consent gaining training

Review the delivery methods you have in place for gaining consent. Consider the following:

- Agents should be provided with the consent statements that have been provided by their own organisation or their clients' organisation
- Role-Plays specifically around the delivery of consent statements
- Playing recordings of 'golden' consent capture conversations
- Asking agents to record and re-play their experiences of giving consent for other brands/channels and rate these experiences
- Provide variations on your consent statements to demonstrate the vital building blocks to make them compliant
- Quiz to sign off show what consent can look like

***N.B of course consent is not the only basis for processing personal data***

ICO guide to processing data



# Summary

Regulatory changes will continue to impact how agents engage with customers in all types of contact centres. We hope this guide has given you some ideas on how and where you could think about focusing your training around the new data protection act.

The below links provide more resources to help you.

- <https://dma.org.uk/gdpr>
- <https://ico.org.uk>
- <https://www.dpnetwork.org.uk/>

For the next few years the data protection act will evolve for you and your customers.

Your DPO, or equivalent will be continually up-dating you on changes.

The Contact Centre Council will always have a slot on the monthly council agenda to review all regulation and how it is impacting marketing, and specifically contact centres.

To read this monthly up-date please visit: [www.dma.org.uk](http://www.dma.org.uk)



# About the Contact Centre Council

The DMA Contact Centre Council actively seek to identify, reinforce, share and shape best practice.

We work with the DMA to support political lobbying in areas that will directly impact marketing in contact centres (e.g. ICO's GDPR & PECR; Ofcom's persistent misuse policy).

We produce best practice guides and valuable materials (the Vulnerable training materials produced by council members are now being used in contact centres in all vertical sectors).

We work on initiatives to support the needs of DMA members and the council.

We debate, attend events, run events, conduct research and go to the pub after every monthly meeting.

If you would like to understand more about the work of the Contact Centre Council please email [ccc@dma.org.uk](mailto:ccc@dma.org.uk)



# About the DMA

The DMA is the professional association representing companies working in the UK's multi-billion pound data-driven marketing industry. Its vision is to create a vibrant future for Britain by putting 1-to-1-to-millions communication at the heart of business, even society: promoting organisation-customer relationships that are genuine, in touch with the individual's needs, inspiring, helpful and mutually beneficial.

It provides members with the strongest framework for driving success: the DMA code, unlimited legal advice, political lobbying, business-critical research, educational and networking events, niche tools and resources, the latest and most creative thinking and the greatest community of digital and direct marketing experts, leaders, shapers and creators to support and inspire.

For further information: [www.dma.org.uk](http://www.dma.org.uk)





# Copyright and disclaimer

DMA advice: GDPR - a training guide for contact centre agents is published by The Direct Marketing Association (UK) Ltd Copyright ©Direct Marketing Association. 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 permission of the DMA (UK) Ltd except as permitted by the provisions of the Copyright, Designs and Patents Act 1988 and related legislation. Application for permission to reproduce all 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 advice: GDPR - a training guide for contact centre agents, no liability or responsibility of any kind (to 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 2018. All corrections should be sent to the DMA for future editions.