DMA advice: Social media, the GDPR and data

20 things you need to know

Published by the DMA Social Media Council

Contents

Acknowledgements

The DMA would like to thank members of the DMA Social Media Council for their contribution to this guide, in particular:

Laurier Nicas Alder, ***TMW Unlimited***
Julie Atherton, ***Small Wonder***
Sam Beament, ***Dyson***
Milly Bellotti, ***Collider***
Hannah Bland, ***Aviva Investors***
Joel Davis, ***agency:2***
Ben Dunham, ***Osborne Clarke***
Nick Joy, L***V=***
Sally Rushton, ***Jaywing***
Lynsey Sweales, ***Social B***

Introduction: Social media, the GDPR and data

Don't be afraid to handle your social media data after the implementation of GDPR.

Social Media can be the perfect tool for finding out what your consumers want from you and how they feel about your product.

The DMA's Social Media Council have collated exactly twenty things you need to know about social media in relation to GDPR that they have encountered in their everyday work about social data to help you and your business.

GDPR aims to put the consumer at the heart of every business and with social media being used as a direct way for your customers to talk to you and give you valuable feedback, it's important you keep this social data protected and handled appropriately to keep your customers happy.

Social media, the GDPR and data: 20 things you need to know

Community management

a) Public messages

Personal data exchanged in public messages on social platforms isn't owned by the brand or agencies acting on behalf of brands, it is owned by the individual social platforms.

The social platforms have their own privacy policies and guidelines which social platform users and advertisers agree to comply with. The brand must set out in its privacy policy/ data collection notice how it will use such information in accordance with the requirements of the GDPR , in particular but not exclusively the right to be informed:

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

An example of this is the Information Commissioner's Office Social media section in its privacy policy:

https://ico.org.uk/global/privacy-notice/how-you-can-contact-us/

If you are running a competition on a social media platform and collecting personal information then how you are going to use that personal information in the future needs to be set out in the competition entry terms and conditions and on the competition entry form?

If a brand or an agency acting on behalf of a brand is moderating these channels then the staff members of the brand or agency working on behalf of the brand must carry out the moderation in line with the brand's social media policy.

The moderator should suggest to the social media user that it might be better to use direct messaging rather than public messaging if personal information is going to be shared via public messaging.

If the user persists in sharing personal information via public messaging then in addition to the data collection/ privacy notice the moderator should use boiler plate clauses for public messages where personal information is disclosed, for example customer service issues

Something short that can be personalised to the tone of the conversation is best. See as follows:

> Thank you for your message.
>
> We care about the security of our consumers, so please note that we will not use any of your personal details obtained in this communication for marketing purposes.
>
> If you provide us any contact information for customer service purposes, it will only be used to manage your enquiry and will not be used for any other reason.

Any personal information shared in public by the user on social platforms is done at their own risk.

Social media users may not realise the consequences of sharing such personal information on the platform via public messages and an organisation cannot infer that a user has consented to the use of that personal information for any purpose.

Despite this, we'd recommend moderating the platforms to delete (where possible) any information that you believe that they have shared in error or without realising the consequences and/or encourage them to use direct messaging instead as above.

b) Private messaging

The same points as in respect of public messaging/ are equally applicable to private messaging.

Brands or agencies acting on their behalf should not do anything with personal information disclosed in private messages which the sender of that message would not expect.

How will private message advertising be affected by GDPR?

On Facebook there is the option for messenger to part of your ad placements or for you to solely advertise by conversations through Facebook messenger.

If you choose your audience through lookalike audiences, the social media platform is the data controller and therefore will handle the responsibility of ensuring platform users have opted in/consented to receive lookalike audience marketing messages.

However, if you are using a custom audience built from your customer data, you must ensure that you have adhered to GDPR requirements.

In particular you must have told your current registered customers and registered prospects in your data collection/ privacy notices then if they are on a social media platform you will use the contact details you told about them and combine this with information which the social media platform holds to find their social media platforms account handles.

Facebook will launch a tool which will require advertisers to certify that they have consent before uploading email addresses of their registered customers and prospects through Custom Audiences although not much is known about how this will work in practice yet.

Whether B2B or B2C if we have an individual's details it falls under GDPR, are there any differences we should be aware of?

The GDPR only applies to personal data and not to information about organisations.

Contact details of a staff member of an organisation, such as name, job title, phone number email address, personal social media handle all fall within the definition of personal data.

The only exception to this is generic email addresses such as sales@dma.org.uk, unless you know the individual staff member who has sole access to a generic email address.

If the individual staff member's details falls within the definition of personal data in the GDPR then any organisation must process that information in accordance with the GDPR and the individual staff member has all the data subject's rights under the GDPR.

Information about organisations - for example details of how many staff members it has - is not personal information.

A B2B website has their teams direct email address and telephone number to contact them for enquiries will this still be ok to use for prospect purposes after GDPR?

GDPR applies to personal data – this includes individual staff members contact details within a business.

However generic email addresses such as legaladvice@dma.org.uk and generic telephone numbers attached to a team will fall outside the definition of personal data.

In this situation, you would, of course, be allowed to use these contact details to contact the person if you were

interested in their services, what you would not be allowed to do is contact the person about selling your services (as in cold contact).

For prospecting purposes, the way to continue this work would be to carry out your research on an organisation but then contact their main contact number or general email address and contact them that way.

How do you deal with custom audiences on platforms following GDPR

A custom audience from a customer list is a type of audience that you can create on a social media platform made up of your existing customers.

In order to create the list, an advertiser must share customer data (usually email, but phone numbers can be used too) in order for the platform to match it with their database.

A crucial part of this process involves the scrambling or 'hashing' of data so it is obscured, but is still unique enough to be matched.

Once matched, the advertiser will be able to target its customers on the list with adverts whilst they're using the platform.

Creating a custom audience can be extremely effective, especially if an advertiser segments their list prior to the upload. In this case the advertiser must state in their data collection/ privacy notice that it will use information it holds about its customers to find and contact them on social media platforms.

Facebook is shortly introducing a Custom Audiences Permission Tool which will require advertisers to confirm that proper consent under the GDPR has been obtained for the personal information they upload to create Custom Audiences.

If a privacy policy doesn't already include a statement that it will use information it already holds about them to find them on social media platforms in its data collection/privacy notices then it will need to do so.

The data collection/privacy notice must be updated in a language that can be easily understood, explaining how the data will be shared with social media platforms and that this will be done on the consent legal basis.

In addition, or alternatively, advertisers can use the data to create 'lookalikes', which will expand their audience exponentially to include people that display similar traits to the customers in the original upload.

In the case of creating lookalikes there is no need for the advertiser to get the consent of its customers since the advertiser is not targeting them – indeed existing customers will be specifically excluded from the lookalike list.

What needs to be considered under the GDPR?

The handling of any personal data should always be taken seriously, especially as GDPR brings with it significant consequences for non-compliance, including fines of up to €20 million or 4% of a company's global turnover.

Organisations must have a legal basis for processing personal information under the GDPR and as we have seen above Facebook's new Custom Audiences Tool requires advertisers to get consent before uploading personal information to Facebook to create Custom Audiences.

In terms of the social media platforms in the case of creating lookalike audiences, they are able to do this based on the user's relationship with the platform.

The user will have agreed to receive lookalike advertisements when it signed up to the social media platform.

If a platform user responds to a lookalike advertisement then once the user goes back to the advertiser's website the advertiser is responsible for compliance with the GDPR in particular the advertiser must make sure that it complies with the right to be informed under Article 13 of the GDPR.

[1] Reference – Articles 13 & 14 of the GDPR.

Retargeting ads – where will we stand on running these?

Retargeting allows you to serve adverts to people who have visited your website.

A pixel is placed on your website which is invisible to visitors and places a unique cookie in their browser which allows them to be identified as having visited your site.

Under the Privacy and Electronic Communications Regulations as amended you must be obtaining consent to use these types of cookies – please see:

https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf.

Please note that implied consent does not exist under the GDPR and you cannot use the legitimate interest legal ground under the GDPR for these types of cookies.

You will have to ensure that your consent for the use of re- targeting cookies meets the higher GDPR standard of consent:

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

The current cookie law derives from a piece of European legislation called the ePrivacy Directive.

This is currently being revised and will become the ePrivacy Regulation, once it has completed its passage through the Brussels legislative process. We expect this to happen in late 2018 or early 2019.

There will almost certainly be major changes

Can businesses link their social channels via email and their website under GDPR?

Yes, businesses will still be able to link to their social channels via email and their website, and encourage people to connect with them on these platforms.

However organisations will have to explain in their privacy policy/data collection notice how they will use social media contact information.

The organisation should also ensure that it has an internal social media policy detailing how staff members should respond to social media.

Profiling

Businesses often leverage data about an individual from a number of sources, including:

- Social media profiles (in order to better understand a person's demographic location)
- Personal characteristics and/or interests

As with any processing of data under the GDPR, in order to do this, a lawful basis for collecting and using this data must be established.

For more information read the DMA GDPR guide on profiling:

https://dma.org.uk/article/dma-gdpr-guidance-profiling

If a business identifies a "superfan" (customer), would a business be allowed to reach out to them via social media touch points?

A business may be allowed to reach out to them via social media touch points in the following scenarios

a) If the superfan is already a customer of the business

The business should have already given the superfan the required information under the right to be informed under the GDPR when they became a customer of the business.

The business must have told the superfan that it would send marketing messages and/or contact them via social media touch points.

In addition, the business would have to have a legal ground under the GDPR for reaching out to the superfan- the two most likely legal grounds are consent and legitimate interest.

Under the Accountability principle under the GDPR it will not record the reasons why it chose the legal ground as well as the decision to use that particular legal ground.

b) If the superfan is not already a customer of the business

The business will need to give the superfan the required information under the right to be informed under the GDPR.

The business would need to tell the superfan that it will contact them with marketing messages and/ or contact them via social media touch points.

In addition, the business would have to have a legal ground under the GDPR for reaching out to the superfan- the two most likely legal grounds are consent and legitimate interest.

Under the accountability principle under the GDPR it will not record the reasons why it chose the legal ground as well as the decision to use that particular legal ground.

Social media reporting and storing

Social media reports are used to track performance against KPIs and provide insight for future campaign development.

Tracking performance

- Data for social media reports can come from a variety of sources including Google Analytics, in-app analytics or dedicated reporting tools. The data is usually held in a bespoke spreadsheet and is used to create table or charts to highlight the results.
- Typical measures included in the reports are shares, likes, conversions, sales, engagement rates, reach, follows, clicks
- As the data is held at an aggregated level it falls outside the definition of personal data in the GDPR and therefore this type of social media performance can continue to be reported in the same way post GDPR

Providing insight

- Social media reports can include example comments or screenshots of posts that provide insight on sentiment and opinion. These posts will fall within the definition of personal data in the GDPR but are publicly available to view on the social media platform.
- The posts can be included in a social media report post GDPR as a link to the location on the social media platform
- If a screenshot of the post or comment is included it should be anonymised
- The advertiser will have to think carefully about the purpose for which it uses this personal information.

- For example it cannot use the personal information in the post to send direct marketing to the platform user unless the platform user has already agreed to receive direct marketing from the advertiser

What is permissioning? How to permission or re-permission? What are permissions in social media and how will they apply?

Organisations should have decided before the 25 May 2018 as to which legal ground under the GDPR they were going to use for their direct marketing activities.

There were six possible legal grounds under the GDPR and there is no hierarchy of legal grounds - an organisation just needs one legal ground.

The two most common legal grounds for direct marketing are consent and legitimate interests. For more information on these two grounds please see the DMA GDPR Guide at:

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

If brands are using the consent legal ground then they need to be aware of the ICO guidance advising that the consent should be revalidated once every two years under GDPR, showing an intention to ensure that consent isn't assumed to last for a long period:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

For the consent legal ground to work well, brands need to be more imaginative than they were with the cookie acceptance box, which offered no choice and frequently just got in the way.

Many are using the consent process more creatively, and so, instead of bluntly asking people if they want to consent to receive more communications, consent should be presented as an opportunity to engage with the brand whilst at the same time confirming in the consumer's mind why they should consent.

Using the consent legal ground as the legal basis for direct marketing carries some risk including the risk of a complete opt out from all channels because the recipient does not respond, low response rate etc

The DMA UK advise strongly advises organisations to consider using the legitimate interest legal ground as a basis for their direct marketing by postal mail to avoid the risk of a complete opt –out from all marketing channels because a customer does no respond to the request for consent.

The DMA would also advise organisations to carry out testing of the wording of consent requests to ensure they chose the wording which has the greatest response rate.

The exercise needs to be as user friendly as possible to achieve the highest number of customers consenting to receive direct marketing whilst being conducted within the law.

What are permissions in social media and how will it apply?

Thanks in part to the recent Cambridge Analytica case alongside GDPR, social media platforms have invited users to agree to new terms and conditions of use and also to review their individual user settings on the platform with regard to visibility to other platform users.

This in turn effects permissions for ad networks and the brands wanting to advertise on social media platforms either through paid (see our earlier notes on custom audiences) or organic activity.

For users of a social media platform who like or follow a brand's page on a platform there will not be much change as the user agrees to engage and be part of that brand's community on the platform.

However, if the brand wants to use the personal information collected via the platform to contact the user other than via the platform they will have to make this very clear in the brand's data collection/privacy policy and find a legal ground under the GDPR for the use of this personal information.

Brands also need to be aware that the ePrivacy Directive is currently being revised and will become the ePrivacy Regulation.

It is currently going through the Brussels legislative process and is expected to be passed in late 2018 or early 2019.

It is not known at the moment when the new Regulation will come into force. One important point to note is that over the top services run by many social media platforms will come under the scope of the new Regulation.

Cybersecurity and training

The obligations regarding the security of personal information held by a brand and cyber security have not really changed much under the GDPR.

The security principle in the GDPR requires organisations to process personal data securely by taking appropriate technical and organisational measures to protect the personal data.

For more on the security principle please see:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

It is important that all staff members of an organisation are trained in data security measures appropriate to their job role. The Government Cyber Security Essentials website contains some good advice particularly for small organisations who may not have a dedicated IT security team:

https://www.cyberessentials.ncsc.gov.uk/advice/

If your organisation has an IT security team then cyber security and training will be primarily their responsibility. All organisations - no matter what the size - should be aware of and should put the following basic cybersecurity items in place (this is not an exhaustive list):

- Storing all client/customer personal data and other confidential in a CRM system that is both secure and encrypted
- All CRM and systems where personal data or other confidential information is stored is password protected (passwords should be secure passwords – read for further info:
- https://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care/
- Your network should be secure – there should be sufficient security and firewalls in place so that cyber-attacks can be limited and if there is a cyber-attack its effects can be limited
- You have anti-virus software installed / in place on every computer and device where your team access data
- As well as technical and organisational IT security your all staff members should be trained to be 'cyber aware'.

Most cyber-attacks start with someone within an organisation replying to a cyber-attack phishing email – these emails will often appear to have been sent from a member of the senior management team of an organisation whose email account has been hacked/compromised.

If the email is opened or the attachment downloaded – this could expose the organisation to a full-blown cyber-attack or ransom ware attack.

To help limit the chances of this happening it's not only important that you have the correct security on emails in place but also have your team trained.

Your team members need to follow the advice of your IT security about using unsecured Wi-Fi networks (such as publicly available wi-fi networks in coffee shops and other places); what personal information and business

confidential information you can transmit when using such networks; and any additional security measures staff members should take.

Please see:

https://ico.org.uk/media/fororganisations/documents/1575/it_security_practical_guide.pdf

In conclusion, review your cybersecurity within your organisation and upskill the level of cyber- security knowledge with every staff member in your organisation.

These measures won't prevent a cyber-attack but they should limit the consequences of a cyber-attack.

Are there any particular GDPR considerations for our employee advocates using social media?

Absolutely, though there are not many changes from the way your employee advocates should have been using social media under the old data protection legislative framework.

Most of (if not all) your social media activity takes place on a third party platform and the user will have already accepted the platform's privacy policy and terms and conditions of use.

Their relationship is with the platform provider, not your organisation: staff members of an organisation who are social media advocates need to have a good working knowledge of each platforms' rules so they do not break them when they are promoting an organisation on a particular platform.

How personal information is presented or stored on a particular platform is the responsibility of the platform owner. Staff member advocates working on behalf of an organisation need to comply with the organisation's social media policy.

Staff member advocates need to have GDPR training so that they know that if the organisation they are working on behalf of takes some personal information from a social media platform, and it uses such information on its own account then the organisation - not the social media platform - will become the controller and be responsible for GDPR compliance.

For example, if we were to take some personal information from a Twitter post and store it in a spreadsheet or in an email then we would be liable for making sure that the personal information was being stored securely, was accurate, and held for no longer than necessary to achieve the purposes.

The organisation would also have to find one of the six legal grounds under the GDPR as its lawful basis for processing the personal information and then give the author of the Twitter post the required information under Article 14 of the GDPR.

Will you still be able to collect personal data via lead generation forms (including third party i.e. Twitter cards)

a) Twitter cards

Yes, you will.

The brand who has posted the Twitter card will still be able to get access to information about who has clicked on it through Twitter based on the platform's data collection notice and terms and conditions.

However, if the call to action in the Twitter card is to direct users to click on a link to your website, when they land on it. If you are using cookies on your website you will need to explain this on your website and depending on what you are using the cookies for, either get consent or use the legitimate interest legal ground under the GDPR.

Organisations must have a legal basis for processing personal information under the GDPR. If you are collecting personal information on the website then you will need to explain to visitors the purposes for which you are collecting

the information.

GDPR legislation stipulates that personal data must be collected for "specified, explicit and legitimate purposes". Therefore when personal information is collected, website owners must firstly explain to visitors how it will be used and provide them with their information rights, and secondly ensure the different purposes for processing the personal information are separated out.

Regarding the first point, it's up to the website owner to specify in the data collection form in what way the personal information will be used and ensure it is not ambiguous so for example instead of saying "marketing purposes", using wording such as "information and deals on new and current products".

On the question of separating consent for different purposes, website owners need to ensure that they are not grouping different purposes in one place so that users are able to select one purpose but not the other.

b) Third party lead generation forms

You will still be able to collect personal information via third party lead generation forms under the GDPR.

However, if you are collecting email addresses, mobile numbers for mobile marketing or social media handles to pass on to third parties, the lead generation company collecting the information can only do this using the consent legal ground under the GDPR.

The lead generation company will also have to name the third parties it wants to pass the information on to individually by name.

Organisations need to remember that consent to pass information on to third parties is a one step process. So the third party who has received the personal information from the lead generation company cannot rely on the original consent given to the lead generation company for the third party to pass the personal information on to other third parties.

The third party will need to carry out the due diligence on whether the lead generation company has correctly collected the personal information using the checklist in the ICO Direct Marketing Guidance for buying a marketing list in the Lead Generation and Marketing list section at:

https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

If you are a first party collecting personal information from a customer and want to pass it on to third parties for lead generation then you must separate out the two purposes of first party marketing and third-party marketing.

In addition, you must comply with all the other requirements of the GDPR – please see:

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

The right to be forgotten

The GDPR grants various rights to data subjects.

One of these is the right to request erasure of their personal data, also known as the right to be forgotten.

The right is not absolute - it can only be exercised is certain situations.

See the ICO Guide to the GDPR on the right to erasure:

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

If a business runs a multi-national campaign from the UK to countries outside Europe, would it be correct that this wouldn't sit within the GDPR regulations?

Now that the GDPR is in force, brands carrying out ad campaigns are (or at least should be) all too aware of the importance of complying with the GDPR - insofar as the campaign will involve the collection, storing and/or use of personal data which identifies an individual.

However, one common misconception is to do with the applicability of the GDPR when brands based in the UK run multi-national campaigns which collect the personal data of individuals based outside the EU.

"We're picking up data relating to people outside Europe, so the GDPR doesn't apply, right?".

Wrong.

The GDPR applies to "the activities of an establishment of a controller or processor in the Union".

In other words, the deciding factor is whether the party running the campaign is based in the EU, not the location of the data subjects. If the social campaign is being arranged from the UK by a UK brand (or a UK subsidiary of a global brand), all personal data processed as part of that campaign will need to be treated in compliance with the GDPR, even if the campaign is targeted at individuals in, say, Australia.

As such, the usual GDPR considerations such as having a lawful basis for processing personal data, ensuring appropriate security mechanisms are in place and transferring personal data outside the European Economic Area (EEA0 – the 28 Member States of the EU plus Iceland Lichtenstein and Norway) only when recognised protections are in place will apply to any personal data obtained as part of the social campaign.

Of course, if the campaign is such that no personal data is processed by the brand running it then the GDPR would not apply in any event (such as targeted banner ads served using a social media site's own targeting capabilities where the brand does not come into contact with, or take controllership of, end user data).

In some ways, this can make things simpler for advertisers.

Rather than having to treat different personal data sets from social campaigns differently, depending on the location of the target audience, a uniform worldwide policy can be adopted which meets the GDPR standard.

That said, advertisers should also be aware that the use of personal data relating to an individual in a country outside the EU may also engage that country's own data protection laws.

As such, it is worth carrying out a local assessment in each case to check that the GDPR-compliant measures in place are sufficient to adhere to the relevant local rules.

Celebrity and brand accounts: If a business wants to work with them on campaigns to reach their audiences, will any new factors need to be taken in to account to still run campaigns this in the future?

Unless you are asking for any personal details from the audiences - such as email or phone number - the rules for celebrity/brand relationships remains the same under GDPR.

This includes clear labelling of sponsored posts so that audiences are aware that it is a paid promotion.

If you are running a competition with an influencer or celebrity in which you require personal details from entrants, whether at entry stage or to contact winners, you need to ensure any handling of this data is GDPR-compliant.

Further details on competition handling can be found at question 22 about competition draws.

The rules for celebrity brand relationships are part of the CAP Code and guidance can be found at:
https://www.asa.org.uk/advice-online/celebrities.html

What sort of data from social media reports can we retain and use, considering that it has been generated from a third party platform?

As discussed, the processing of personal information that takes place on a social media platform is ultimately the responsibility of the platform provider.

They will have required users to sign up to their terms and conditions of use and their data collection/privacy notice.

If the user agrees to these terms and conditions of use, and the data collection/privacy notice, then it's up to that platform owner to ensure that the personal information held on the platform is processed in compliance with the GDPR.

However, the situation changes when a brand or agency acting on behalf of a brand uses a software tool to interrogate the platform(s) to extract personal information.

By removing that personal information from the original platform on which it was published, the responsibility shifts to us as we become controllers.

Accordingly, we have to treat that personal information in the same ways as any other personal information under the GDPR.

Ultimately you will have to comply with all the legal requirements under the GDPR including but not limited to making sure you have a legal ground under the GDPR for processing such personal information; a valid purpose as to why you are retrieving the personal information from the social media platform; and being able to justify your actions under the accountability principle.

If you are storing the personal information, you need to ensure it is accurate and kept up to date.

You must only keep the personal information for as long as it is necessary for the specified purposes.

As an example, you might run a report every month using your social media monitoring tool to measure sentiment. In this case, it's fine to run the report so that you can aggregate the total results (as this isn't giving away personal information).

If you export a spreadsheet with all the posts on it from a social media platform on it (highly likely to contain personal info), ask how you'll store it: do you really need it at all?

Will competition draws such as like a page, like this post and share with your friends, tag a friend be able to run?

The way you run competitions using "like a page" or "like this post" doesn't need to change, if you adhere to the platforms' terms and conditions.

You should bear in mind CAP's concerns about using these methods:

https://www.asa.org.uk/advice-online/promotional-marketing-prize-draws-in-social-media.html

It is doubtful whether you can use share with your friends and tag a friend as an entry mechanic to competition draws because of the higher consent standard under the GDPR nod the fact that implied consent does not exist under the GDPR.

It would be difficult for the promoter of the prize draw / competition to argue that the person referred or tagged had consented to receive marketing messages from the promoter.

You will have to ensure that how you collect and process personal information collected during entry to the prize draw/competition is compliant with the GDPR.

You will have to ensure that entrants are given the required information under the GDPR – please see:

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

The promoter will also have to ensure that they meet their accountability requirements under the GDPR and have appropriate policies and procedures in place such as data retention.

Is there anything a business needs to bear in mind on dark social going forward?

Dark social describes the social sharing of content that occurs outside of what can be measured.

By web analytics programmes this occurs when a link is sent via online chat or email rather than via a social media platform – i.e. Techopedia.

Referrals from dark social are counted as direct traffic and this makes it difficult to measure social media as a whole.

This will remain unchanged when GDPR comes into play as the referral source is anonymous.

Conclusion: Social media, the GDPR and data

From how B2B and B2C can be shaped by social data to the use of third party platforms, social data has proven to be not as scary as first thought.

GDPR is an opportunity to find who in your audience are the most engaged and using social data can be a great advantageous tool to do this.

Careful thought and clever strategy can ensure you get the engagement you want and a happy audience to go alongside this.

Different social media platforms can offer different avenues to success so next time you want to run a campaign, keep these questions in mind to help you get the best results you can.

About the DMA Social Media Council

Social media offers you huge opportunities in real-time marketing and improved customer service through unrivalled opportunities for customer engagement with a wide range of audiences.

The DMA's Social Media Council promotes the use of social media and aims to help you keep up with the latest developments and take full advantage of the creative and targeting opportunities.

The council works to produce detailed and insightful research, host informative events, advise on legal and resourcing issues and to enhance DMA members' understanding of how to optimise their return on investment using social media.

To help shape the future of social media marketing, contribute to the discussions here or email socialmedia@dma.org.uk to find out more about the council and its work.

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