Answering your Data Protection 2016 questions

At the Data Protection 2016 conference you kindly sent in a large number of questions for our speakers and panel members, but we could not get through them all on the day. Our legal team has been through the questions that got away
We received so many questions that we have split them up by theme.

Contents

Right to be forgotten

Right to be forgotten -- how do you see this working in practice, across the supply chain, in a consistent and coherent manner?

The right to be forgotten needs to be understood with the right of suppression. If I want to unsubscribe/ opt--out from direct marketing then rather than deleting my information under the right to be forgotten an organisation should retain my information indefinitely and add it to a suppression/opt--out/ unsubscribe file. The suppression file needs to be shared across the supply chain in a consistent and coherent manner by all parties involved.

If the right to be forgotten does need to be exercised across the supply chain than the data controller has to take reasonable steps to inform other parties in the supply chain who are processing the data subject's information that the data subject has requested the erasure, taking account of technology and the cost of implementing such request in the supply chain.

How does the right to be forgotten fit in for future customer contact regarding safety or product

recall concerns?

Organisations will be able to retain customer information to contact them about safety or product recall concerns even if that customer has exercised the right to be forgotten

Subject Access Requests – is there an expectation these will increase significantly given that the fee will be abolished?
Individuals have the right to obtain personal data held about them by the data controller free of charge the first time. For any further copies of the data the organisation can charge a 'reasonable fee'.
This does not mean individuals will be able to make vexatious subject access requests that damage an organisation. An organisation is within their right to refuse to answer a subject access request, if it is malicious in nature.

If a customer requests deletion of their data, when actioning the request does delete mean total deletion? And what if any data can be retained?

Under the GDPR individuals have the right to have all their personal data removed from a data set. However, if for example, an individual no longer wants to receive direct marketing and asks for their personal data to be deleted then the information should be kept on a suppression file. It is unlikely the text seeks to stop organisations maintaining an in--house suppression file. Guidance will clear up this ambiguity in the future.

Re: Right to be forgotten -- will we have to delete our existing suppression files?

No your own internal suppression files will still be required to make sure you do not contact those people that have asked you not to get in touch. This is a separate requirement to the right to erasure/right to be forgotten.

Right to data portability -- how do you see this working in practice? How will organisations with perhaps limited technical resources be able to respond to this?

The right to data portability only applies where the processing is based on consent, the processing is carried out by automated means and the data subject has provided the information.

In practice it will only apply to cases where the customer switches providers such as social media services or utilities. Organisations with limited technical resources are less likely to have to respond to this

Legacy data -- please can you confirm if the GDPR will be applicable to legacy consents of customers?

Our current understanding is that the GDPR will not be applicable to legacy consents of customers and that there will be some grandfathering provisions. We will have to wait for guidance from the Information Commissioner's Office on this point.

Europe and the GDPR

What impact would Brexit have on UK data protection law and the implementation of GDPR?

If the UK opted to leave it would enter into some form of trading relationship with the EU. Data protection would form part of any such trading agreement. Therefore, the UK would need to implement data protection legislation that was broadly equivalent with the GDPR.
DMA members should continue with their plans to implement the GDPR irrespective of the decision in

the referendum as whatever the result the UK will be moving towards a standard on a par with the GDPR.

The referendum is not a reason to delay plans to understand and become compliant with the GPDR.
Will the GDPR harmonise laws across all member states?

The GDPR will harmonise data protection law in most areas across EU member states. However, there are certain specific areas of policy which permit member states to interpret the law. For example, the age for consent is set at 16 in the text but member states are permitted to lower the level of consent to 13, if they so wish.

The US and the GDPR

Will the Judicial Redress Act really be affordable/accessible to UK citizens?

If a UK citizen has a complaint about the EU--US Privacy Shield then he/she will be able to take the following action before relying on the Judicial Redress Act:

1) Complain directly to the organisation who has signed up to the Privacy Shield

2) Take the organisation to the Alternative Dispute Resolution procedure under the Privacy Shield

3) Complain to the ICO or other national data protection authority

4) Take the organisation to the Binding Arbitration panel under the Privacy Shield

5) Bring and action directly under various US statutes (other than the Judicial Redress Act) and tort law/

What impact will the Apple versus FBI case have on our industry?

The Apple versus FBI case will have very little impact on the UK direct marketing industry as the case will be decided under US law.

The ICO and the GDPR

A question for the ICO and DCMS. Please, clarify what will be included in the ICO guidance roadmap on the GDPR and will DCMS be publishing a similar plan?

The Information Commissioner, Christopher Graham, confirmed that the ICO would be publishing guidance in the future but before they could do that the final text needs to be published in the official EU Journal. Christopher Graham anticipated that would happen in May or June this year.

The Baroness Neville--Rolfe echoed his comments, with both steering clear of giving a firm plan until the final text is published later this year.

Will the ICO have the resources to properly enforce the legislation?

Currently, the ICO is able to charge a fee to organisations registering with them in order to be on the data protection register. All organisations that hold personal data about their staff or customers must register. Under the GDPR the ICO will not be able to charge a registration fee.
The Information Commissioner said that he intends to create a different form of charge in order to

maintain funding for the regulator. The Baroness Neville--Rolfe agreed that the regulator should be funded by the industry but that crucially any charge must be proportionate.

In our industry companies that flout the Data Protection Act and DMA guidelines for example, nuisance calls and high pressure sales, are the fastest growing. Where is the incentive to comply?

We do not have data to support this claim, however; the Information Commissioner and Ofcom are ramping up their enforcement efforts against rogue traders responsible for the majority of nuisance calls. The ICO no longer has to prove substantial harm or distress in order to successful prosecute offenders, making nuisance calls is enough to bring a case forward.

DCMS are going to make caller line identification mandatory for all marketing phone calls, which will make nuisance calls easier to report for individuals. Such measures are having an effect on the rogues. Evidence of this is the increased Telephone Preference Service registrations, indicating more rogues not willing to risk falling foul of the law.
The GDPR substantially increases fines as those organisations that break the regulation can be fined €20 million or 4% of global turnover, whichever is higher. The eye watering fines available to the ICO will be sure to focus minds among the rogue traders.

We are only meant to retain data for "as long as it's relevant". Do you think this definition will be hardened up? What does it actually mean?

This principle has been changed into a storage limitation principle in the new Regulation. Organisations must not keep personal data in a form which permits identification of data subjects for longer than is necessary for which the personal data are processed. This does not apply if the data is being kept for archiving purposes.

The ICO has produced guidance on the current principle: https://ico.org.uk/for--organisations/guide--to--data--protection/principle--5--retention/

The ICO have approached 13 charities as a result of the GoGen media story, encouraging them to make commitments around Opt In ahead the GDPR introduction. How is the ICO not overstepping its remit?

The ICO's response:

One of the organisations we have recently been investigating has agreed to sign up to a best practice model which includes:

- Only contacting individuals who have opted in to direct marketing
- Refreshing consent every 2 years.

This agreement is specific to the organisations business model and our investigation; and would not apply across the board as an official line from the office. Although, we would always support any organisation seeking to instil best practice in information rights across its activities.

However, if other charities are looking to move to this model, we would not deter them from a 'best practice' point of view. The message to the charity sector as a whole, is that they must comply with PECR and there are no caveats for not for profit organisations.

How frequently would the regulator suggest consumer consent should be refreshed, if at all?

The ICO will be publishing new guidance as a result of the GDPR that may add clarity to this. You do

not necessarily have to get a new consent, but you have to offer people the chance to opt out e.g. an unsubscribe on an email message.

With the Red Cross saying that they will only contact individuals who have opted in in the last two years. How does this sit with the 6 months in the ICO guide?

The 6 month rule is only for first use of 3rd party data.

Fundraising

My understanding is that the IoF enforced an opt--in for all charity telemarketing last September. Why is what the Red Cross have announced any different?

Their current code says "Organisations MUST NOT* make direct marketing calls to Telephone Preference Service (TPS)/Corporate TPS (CTPS)--registered numbers unless the person who registered the number has notified the organisation that they are happy to receive calls for the time being".
They also refer to the ICO's direct marketing guidance which is the same advice that would be given by the DMA.

How are the ICO involved in the development of the Fundraising Preference Service?

The ICO are not involved with the FPS. They have publicly said that they don't think it is a great idea and will lead to confusion with other preference services. They will not be responsible for it or enforce it; that will be the job of the charity regulator.
Profiling and automated decision making

Will the new regulation affect profiling individuals using customer data -- would you need explicit consent for traditional profiling internally/with third party?

Yes, the new regulations will affect profiling individuals using customer data.

Under Article 20 of the GDPR individuals have the right to unsubscribe/opt--out from an organisation making a decision--based on automated processing, including profiling, which produces legal effects concerning the individual or similarly significantly affects the individual.

The right to unsubscribe/opt--out does not apply if the decision:

a) is necessary for entering into or the performance of a contract between the individual and the data controller – an example of this would be credit--scoring if an individual applied for a new credit card or an increase in their credit limit

b) is based on the individual's explicit consent

c) is authorised under EU or Member State Law – unlikely to apply to direct marketing

In the case of a) or c) the organisation carrying out the profiling must give the individual the right to ask the organisation to for a human to intervene in the profiling, the right for the individual to express their point of view and the right to contest the decision.

The section on profiling was one of the last to be agreed and therefore we will have to wait for guidance from the Information Commissioner's Office and other national data protection authorities as to the

meaning and what this article covers.

Profiling can be carried out by a third party but you would need to comply with the rules on transferring personal information to a third party in the GDPR.

An organisation carrying out profiling will also have to explain to the individual in their data collection notice/privacy policy whether or not the organisation uses automated decision making and profiling, meaningful information about how the automated decision making/profiling works and how the automated decision making/profiling will affect the individual.

Do we have a clear definition of what processes are deemed to be "automated decision making"?

No, we do not have a clear definition of what processes are deemed to be "automated decision making", however, the Regulation does have a definition of profiling which is defined as automated processing of personal information, which is used to evaluate personal aspects of an individual, in particular predicting or analysing them. The use of an algorithm for such prediction or analysis is a good indication that profiling is taking place.

What do the panel think about the need to get explicit permission to profile people's data and how this affects the ability to deliver a value exchange?

Explicit permission is not required to profile people's data.

People should be more aware of the use of profiling in the value exchange because organisations will have to tell people about profiling in their data collection/privacy policies – see response to Will the new regulation affect profiling individuals using customer data -- would you need explicit consent for traditional profiling internally/with third party. This should help consumers to make a decision about the value exchange.

Consent, legitimate interest and opt--in/ opt--out (B2C)

What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?

Organisations will still be able to use current unsubscribe /opt--out data collection methods for post and telephone direct marketing and for email and SMS marketing if the existing customer/soft opt--in exemption applies under the new regulation as it stands.

This is because direct marketing is specifically mentioned in the Regulation as a legitimate interest and therefore organisations can use the legitimate interest ground as a legal basis for processing personal information.

Organisations will have to provide more information about their direct marketing activities in their data collection notices/privacy policies as follows;

Where the information is collected directly from the individual (Article 14 GDPR)

The identity and contact details of the data controller and the data controller's representative (only applicable if the data controller is located outside the European Economic Area (EEA and has no establishment in the EEA) and the contact details of the Data Protection Officer if the controller has appointed one
The fact that the email address is collected for email marketing The legal basis for the processing

The third parties or categories of third parties to whom the contact details will be passed on to

Any third countries or international organisation to which the marketer intends to transfer the personal data and whether such country has or has not had an adequacy decision made by the European Commission about it
The period for which the personal information will be stored or if this is not possible the criteria used to determine this period
The existence of the following data subject rights in connection with the personal data

a) right of access

b) right to have the data corrected

c) right of erasure

d) right to object to processing of personal information

e) right to data portability

f) if the processing is based on consent the existence of the data subject's right to withdraw consent at any time without affecting any lawfulness of any processing based on consent before its withdrawal

g) the right to lodge a complaint with a national data protection authority

h) whether the provision of personal data is

i) a statutory requirement

ii) a contractual requirement or

iii) a requirement is necessary to enter into a contract and

iv) whether the individual is obliged to provide the data and the possible consequences of failure to provide such data

i) the existence of any automated decision making including profiling and at least in those cases meaningful information about

a) the logic involved

b) significance of such processing

c) envisaged consequences of such processing for the individual

j) if the data controller intends to further process the information for purposes other than for direct marketing, information about that further purpose prior to the processing of such information for the further purpose

The above does not apply if the individual already has this information.

Where the third party obtains the data from the first party (Article 14 a GDPR)

The identity and contact details of the data controller and the data controller's representative (only applicable if the data controller is located outside the European Economic Area (EEA and has no establishment in the EEA) and the contact details of the Data Protection Officer if the controller has appointed one

The fact that the contact details are collected for direct marketing

The legal basis for the processing

The third parties or categories of third parties to whom the contact details will be passed on to

Any third countries or international organisation to which the marketer intends to transfer the personal data and whether such country has or has not had an adequacy decision made by the European Commission about it

The period for which the personal information will be stored or if this is not possible the criteria used to determine this period

The existence of the following data subject rights in connection with the personal data

a) right of access

b) right to have the data corrected

c) right of erasure

d) right to object to processing of personal information

e) right to data portability

f) if the processing is based on consent the existence of the data subject's right to withdraw consent at any time without affecting any lawfulness of any processing based on consent before its withdrawal

g) the right to lodge a complaint with a national data protection authority

h) the first party source from which the personal data originate and if applicable whether it came from publically accessible sources

i) the existence of any automated decision making including profiling and at least in those cases meaningful information about

a) the logic involved

b) significance of such processing

c) envisaged consequences of such processing for the individual

j) The controller (third party) must provide the above information within the following time limits

i) within a reasonable period (at the latest within one month) having regard to the specific circumstances in which the data are processed or

ii) at the latest of the time the third party sends the first email to the individual or

iii) at the time of disclosure to a second third party if disclosure to a second third party is envisaged

i) if the data controller intends to further process the information for purposes other than for email marketing information about that further purpose prior to the processing of such information for the further purpose

The above does not apply where

a) the individual has this information already

b) the provision of such information would involve a disproportionate effort (unlikely to apply to email marketing)
c) obtaining or disclosing information is expressly laid down by EU or national law or

d) where the information must remain confidential subject to an obligation of professional secrecy regulated by EU or national law.

Can you provide some clarity around consent, the difference between 'unambiguous' consent and 'explicit' consent and confirm the opt--in/out rules?

"Explicit consent "was only re--introduced into the text of the Regulation right at the end of the negotiations and therefore there is no definition of it in the current text.

"Unambiguous" consent is defined in Recital 25 of the Regulation as " a clear affirmative action establishing a freely given, specific informed and unambiguous indication of the data subject's agreement to personal data relating to him or her being processed , such as by written including electronic, or oral statement.

This could include ticking a box when visiting an internet website, choosing technical settings for information society services or by any other statement or conduct which clearly indicates in this

context the data subject' s acceptance of the proposed processing of their personal data. Silence, pre--ticked boxes or inactivity should therefore not constitute consent.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be granted for all of the processing purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

If you are using the legitimate interest ground as the legal basis for direct marketing then the opt-- in/ opt--out rules will not change once the GDPR comes into force. You will have to note the new information requirements as discussed above in the response to the question **What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?**

Could the panel give some examples of and clarification on when direct marketing constitutes a legitimate reason for contact without consent?

There are two legal bases for sending direct marketing under the Regulation, consent and legitimate interest. If you chose the consent route this will have to be done on a subscribe/opt--in basis, if you chose the legitimate interest route this this can be done on an unsubscribe/opt--out basis. Direct marketing is specifically stated in the Regulation to be a legitimate interest. If you go down the legitimate interest

route then you will have provide an unsubscribe/opt--out process and comply with the new information requirements as discussed above in response to the question **What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?**

Can you email people for whom you don't have consent, in order to gain opt--in, explicit consent?

No, you cannot. The only exception to this is if you are emailing people to ask if they want to change their mind and subscribe/opt--in to email marketing. The email must be a customer service email and contain no marketing material at all. You will have to treat those who do not respond as remaining unsubscribed/ opted--out. You can only treat those who respond and positively subscribe/opt--in to email marketing as being eligible for email marketing in the future.

When we engage new clients, will it be possible to take acceptance of our terms of engagement as consent to send info to contacts in the organisation? How do you believe we can now gather third party consent?

Under the Regulation, it will not be possible to take acceptance of your terms of engagement as consent to send information to contacts in the organisation. Consent to direct marketing must be separate from acceptance of terms and conditions.
We believe that you may be able to gain consent for third party marketing for post and telephone using the legitimate interest route provided the information requirements are met – please see response to the question, **What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?**

We will have to wait for the Information Commissioner's Office to confirm this. You will still need to screen against the Mailing Preference Service and the Telephone Preference Service. The rules on third party consent under the Privacy and Electronic Communications Regulations for email and SMS marketing remain the same.

Does the GDPR kill third party data?

The third party data industry has been pushing the limits of legislation for some time. The appetite of businesses for personal data has meant that data companies have gone to greater lengths and become used less scrupulous tactics to gather people's details. Those companies that can adapt and legitimately persuade people to opt in to truly relevant messages from companies they want to hear from will survive, but the old model of "we may pass your details on to carefully selected third parties" is on its way out.

Consent, legitimate interest and opt--in/ opt--out (B2B)

How will the changes with the implementation of the GDPR impact on B2B marketers differently to B2C marketers?

The difference in effect between B2B and B2C one--to--one marketing is going to be small. This is because B2B data can also be viewed as personal data as it identifies an individual. A business email or phone number relates to the individual and is therefore considered personal data. In practical terms this means B2B and B2C will be in a similar place as most are dealing with personal data for their one--to--one marketing.

Please can you clarify the situation regarding email, telephone and fax direct marketing for B2B purposes? Which will be opt--in and which will be opt--out?

Please see attached grid.

	B2B	
	Own marketing	3rd party marketing
Mail	opt-out	opt-out
Telephone	opt-out	opt-out (TPS/ CTPS screening)
Email	opt-in (unless corporate subscriber exemption)	opt-in (unless corporate subscriber exemption)
SMS	opt-in	opt-in
Fax	opt-out	opt-out (FPS screening)

In terms of consent will B2B contacts be treated the same as B2C especially in terms of email?

B2B contacts will be treated the same as B2C if personal data is involved. The rules on email marketing are not being changed by the GDPR except for the information requirements as discussed above in the response to the question **What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?**

In the B2B market will we see contacts inundated with calls for consent as companies try to get their data compliant therefore having a negative impact?

No, because companies will not have to make calls asking for opt--in/subscribe consent.

How does consent apply to purchased data lists, will we now need to seek opt--ins for cold call lists in B2B?

No, you will not need to seek opt--ins for cold call lists in B2B. the rules will remain the same except for the information requirements as discussed above in the response to the question **What changes would be required to current opt--out consent data collection methods under the new regulation as it stands?**

Cross border data transfers

How are cross--border data transfers to non--EU markets covered by GDPR?

The GDPR makes it clear that it will apply to processing of personal data about EU citizens no matter where in the world the processing takes place.

Transfers of personal information to markets outside the European Economic Area (28 Member states of the EU plus Iceland Lichtenstein and Norway) will only be permitted if 1) the market has been held by the European Commission to have an equivalent level of data protection legislation to the EU or 2) Model contract clauses are used to cover the transfer or 3) the transfer is internal to an organisation who has had Binding Corporate Rules approved.

Relationship between GDPR and the Privacy and Electronic Communications Directive

Do the new regulations include the soft opt--in?

The existing customer/soft opt--in exemption for email and SMS marketing is contained in the Privacy and Electronic Communications Directive which is a separate piece of legislation. The European Commission will revise this Directive once the GDPR has completed its passage through the Brussels institutions.

The regulations will not change the existing customer/soft opt--in exemption for email and SMS marketing apart from changing the information requirements please see response to the question

Vulnerable consumers

How do businesses protect the vulnerable? How does the ICO define vulnerable?

We are not aware that the ICO has a definition of vulnerable; it is a difficult thing to classify. It may include older people or people who are unwell, but it might also include temporary conditions such as bereavement.

The DMA has done a lot of work on this subject and has published guidance for contact centres to help them http://dma.org.uk/article/white--paper--guidelines--for--call--centres--dealing--with-- vulnerable--consumers

DMA Group guidance

Will there be more regional events, not just London--based ones for the GDPR updates? Or will there be an ability to attend online over video link?

There will be a series of regional events covering the GDPR. The legal updates will now have a focus on the GDPR and will be taking place in Bristol for the West; Leeds or Manchester for the North, and Edinburgh or Glasgow for Scotland.
The DMA will also be hosting a series of webinars on the GDPR, which will be free for DMA members to watch online and ask questions.

Will the ICO offer courses or 'official' training on DP?

The DMA Group will be offering training and guidance. The IDM has a new 1--day GDPR course with Rosemary Smith from Opt--4 and a new online award. The DMA will be offering bespoke consultancy to organisations in the future.

How does the DMA define excessive marketing -- in terms of an email data list would this be on the data owner or the brand it promotes?

The data owner should define what is excessive, they are responsible for the list and if they value the data they will be careful about over use to avoid excessive opt outs or being classified as spam.
The only way email data can legitimately be used for third party campaigns is through 'hosted mailings' which would be under the control of the data owner. Opt outs from these emails opts the consumer out of further mailings from the data owner not the brand they are promoting.

Should the DMA be doing more to be a consumer facing 'stamp' to show the average consumer that a company looks after their data?

The DMA is a trade association, it is a membership organisation that works for the benefit of the DM industry. If a company acts it accordance with the DMA code and ideals it will have the interests of the consumer in mind.

Consumer education

Would you agree that there needs to be a lot more education of consumers about how data--driven advertising actually funds services and products?

Yes, the DMA agrees that consumers would benefit from more education about how data--driven marketing works. Consumers benefit immensely from the modern data--driven economy and it is up

to brands to be transparent with their customers and consumers how they benefit from data--driven marketing. This is a core principle of the DMA Code, which is 'put your customer first' and this means being transparent and honest.

How can we educate consumers regarding the GDPR and explain the rules in an easy to understand way?

The DMA is a trade association that represents organisations and not consumers. It is up to organisations to educate their customers and the DMA is there to help its members with this process.
The Government and the ICO will be carrying out their own awareness campaigns to ensure consumers are aware of their new rights.

Why have fundamentalists decreased, given the current febrile climate for DP?

The DMA's Consumer Attitudes to Privacy research found that the number of data 'fundamentalists' in the UK had decreased from 31% in 2012 to 24% in 2015. Data fundamentalists are those unwilling to provide personal information even in return for service enhancement.
While the number of smartphone and tablet owners in the fundamentalist segment have each declined by just 3% since 2012, the number of non--smartphone owners and non--tablet owners in the fundamentalist group have declined by 9% and 6% respectively. Young, digital natives are still less likely to be included in this group, but there is no longer the degree of disparity we saw in 2012.
The fundamentalist segment is no longer dominated by tech cautious individuals. Unwillingness to exchange personal information has evolved into a wider societal trend, albeit with waning support.

Right to be forgotten -- how will the consumer know what information is legitimate for an organisation to retain, what information sources are/will be available?

We would hope that the Information Commissioner's Office will issue guidance for consumers on this point.

Is there a risk for business that accidental customer data misuse could result in a Data PPI claim scandal?

It is unlikely to become as big as the PPI issue, but we are hearing more people asking for compensation for having their data misused, or sending invoices to companies for wasting their time. Many of these cases go to the small claims court where they generally find in favour of the consumer.

Will digital tracking techniques need to be more transparent to allow customers to better understand how their data is being used? Or is it a low priority?

Clarity and transparency of consent are a highlight of the new regulations. The DMA would always recommend that an organisation is clear and open about what they do with a person's data -- including digital data such as cookies and other types of pseudonymous data.

We're going to have to market gaining consent in the same way as other goods and services. What ideas do you have to do this effectively?

For some getting information or the latest news from their favourite retailers or publisher will be fine, others will want to see something in exchange such as premium content, special offers, additional services. Make it clear why you collect the data you do and what the consumer will get in exchange; the Guardian's data policy is an excellent example of this.

The DMA Code uses icons successfully. Could we use these icons more widely in relation to data and privacy for consumers?

I think this sounds like a good idea but would require good deal of consumer awareness to gain credibility, the DMA is a trade association not a consumer organisation, these things are usually best left to people like Which?.

Contact preferences

Fundraising Preference Service -- can you provide an update on the proposed FPS and is there any intention for the commercial sector to adhere to the same regulations?

The FPS will be a 'reset button' that overrides any pre--existing opt--ins. It means a consumer will opt out of all charity fundraising communications. If they are a current donor then newsletters, or messages relating to direct debits will be allowed as long as they do not contain fundraising 'asks'.

It relies on the date of opt--out, so if a consumer was to subsequently opt--in to receive information from a charity, that particular organisation would have permission to market to that consumer. If however at a later date the same consumer updated their FPS opt out, that would once again override the charities opt in.

The FPS will not be required by legislation, it will be part of the fundraising regulator's code of practice. People that sign up will only be expecting the service to stop fundraising communications, so it will not be appropriate for other sectors to use it.

Please clarify the required language for Telemarketing Opt--in request. Is it a requirement that the person needs to give you their telephone number in writing?

The ICO's guidance says "The crucial consideration is that the individual must fully understand that their action will be taken as consent, and must fully understand exactly what they are consenting to. There must be a clear and prominent statement explaining that the action indicates consent to receive marketing messages from that organisation (including what method of communication it will use). Text hidden in a dense privacy policy or in 'small print' which is easy to miss would not be enough."

It is not necessary for the person to provide their telephone number as part of the opt--in but it does need to be collected as part of the transaction/data gathering process.

Could you clarify the situation regarding contacting organisations under the new rules, please? If they haven't joined the Business preference service can we call?

I presume this question is referring to the Corporate Telephone Preference Service (CTPS), at the moment the GDPR has left telephone and mail marketing as opt out channels. This means that TPS and CTPS will still need to be used by companies making unsolicited, live sales or marketing calls. If a telephone number is not registered on TPS or CTPS and you want to contact them with a (targeted and relevant) call, you can.