



GDPR for marketers: Consent and Legitimate Interests



Contents

Welcome to GDPR Guidance for marketers	2
Foreword by the Information Commissioner	3
The DMA and the GDPR	4
Introduction:	6
Background:	7
Introducing: Legitimate Interests	10
Citizens' rights and Legitimate Interests	11
Reasonable expectations	13
Legitimate Interest Assessment	14
What questions should you ask?	16
Data Sharing and Legitimate Interests	18
Profiling and Legitimate Interests	19
PECR and Legitimate Interests	20
Introducing: Consent	22
Consent requirements in practice	28
Refreshing Consent	32
Vulnerable consumers and children	35
Using Consent and Legitimate	36
Conclusion	37
Further reading: ICO Guidance	38
GDPR Glossary	39
About the DMA	41
About our partners	42
Copyright and disclaimer	43

Welcome to GDPR Guidance for marketers

The General Data Protection Regulation (GDPR) mirrors the DMA's long-held view about the need to place the customer at the heart of everything we do as marketers. The new regulatory framework takes effect on May 25th, 2018 - and it offers all of us the greatest opportunity for business transformation in a generation, in the context of:

- Put your customer first
- Respect privacy and meet your customers' expectations
- Be honest, be fair, be transparent
- Exercise diligence with data
- Take responsibility, honour accountability

The DMA - supported by our expert partners in government, as well as the Advertising Association in London and FEDMA in Europe, as well as the wider marketing community - has actively influenced the evolution of the GDPR texts since first drafts were circulated by the EU Commission in 2011.

Our advocacy has established vital building blocks within the GDPR that will safeguard the interests of our members and bolster the marketing industry in general. Of particular importance is the clear statement in Recital 47 that "the processing of personal data for direct marketing purposes may be regarded as being carried out for legitimate interests".

We believe that organisations must use the GDPR as a catalyst to transform approaches, balancing privacy with innovation.

To support business transition to this new data landscape, we have crafted a guidance series that examines GDPR through a marketer's lens.

Beginning with *The GDPR for Marketers: The Essentials*, and continuing with in-depth guidance on *Accountability, Legitimate Interest & Consent*, and *Profiling*, this DMA series provides marketers with a framework for innovation and growth.

The guides will help you apply broad best practice principles to your marketing and your customer service approaches. We use live examples and practical advice, linking to new, channel-specific marketing information and tools from around the DMA's member community.

But we must be clear: Article 29 and ICO guidance are general across sectors. There is no established case law, so all guidance will evolve as real-world applications emerge after May 2018.

From boardrooms through to all tiers of organisations, we must work together to create customer-centric business environments. Brands that make data protection a core value will blossom.

Finally, this guidance has been produced with the collaboration of ISBA, the Data Protection Network and the ICO, which have all made valuable contributions.

These partnerships inform our case studies and our guidance with expert insights, establishing a consistent position on the GDPR across the marketing industry.

We hope you find this guidance useful as we move towards a new future in marketing.

Chris Combemale
CEO, DMA Group



Foreword by the Information Commissioner

This is a pivotal time for data protection and privacy.

We have a digital infrastructure that was unimaginable 20 years ago and data protection laws are converging across the globe. Consumer trust is ever more central to both business and the public sector, and a rapidly expanding digital economy is asking more questions of us all.

For me, the end game in the data protection field is always about increasing public trust and confidence in how their personal data is used.

Data protection reforms, including the GDPR, build on previous legislation, and provide more protections for consumers, and more privacy considerations for organisations. But this is a step-change. It's evolution, not revolution.

It's vital that organisations are prepared to comply but they can also prosper in the new regulatory landscape.

If your organisation can demonstrate that good data protection is a cornerstone of your business policy and practices, you'll see a real business benefit.

An upfront investment in privacy fundamentals offers a payoff down the line, not just in better legal compliance, but a competitive edge. I believe there is a real opportunity for organisations to present themselves on the basis of how they understand and respect the privacy of individuals.

This helpful guidance has been drafted by the DMA with its members, members of ISBA and the Data Protection Network with input from the ICO. It will help marketers navigate through the GDPR and complements our own GDPR guidance and additional online checklists and resources.

I hope this guidance helps you be transparent, accountable and ensure people have appropriate control over their personal data.

Elizabeth Denham
Information Commissioner



The DMA and the GDPR



How we create GDPR guidance

The GDPR Editorial Board leads the content direction of the DMA's GDPR outputs. We inform the work with expert advice and guidance from our Responsible Marketing Committee and the specially-appointed GDPR Taskforce.



To generate the right content for the right channels, the GDPR Editorial Board, Responsible Marketing Committee and the GDPR Taskforce work in collaboration with our Councils. This focuses our work onto the immediate needs of the marketers we serve.



Throughout our approach to preparing the industry for the GDPR, we partner with:





What we produce

Our GDPR guidance focuses on the key marketing impacts that May 2018 will bring

GDPR for marketers

The essentials

Accountability

Consent & Legitimate Interests

Profiling

ePrivacy

Information rights

Governed by the GDPR Editorial Board, the Responsible Marketing Committee and the GDPR Taskforce, the DMA's Councils and Committees produce

DMA GDPR advice for marketers

Permission by design

Checklist for trustees

B2B mythbuster

Cloud computing

Action planning

Data governance

All of which we underpin with our events and research calendar, online tools and channel-specific advice and guidance



DMA Events



DMA Research



DMA Insight



DMA Webinars



DMA Guides

Introduction:

**“For in reason, all government without the consent of the governed is the very definition of slavery”
Jonathan Swift, 1724**

Swift’s message is unequivocal: transparency is fundamental. Though the *Gulliver’s Travels* author was referring to the rule of law, his principled categorisation of consent still rings true and has become increasingly relevant to marketers as we inch towards the May 2018 implementation of GDPR.

Key questions have been raised about the way businesses use their customers’ personal data. Who controls it? How is it obtained? How long can it be used for?

Under GDPR, the answer is clear. Data belongs to the individual who is the subject of the data, but companies can use it in the right circumstances, as outlined by six legal bases for processing data:

- Legitimate Interests - where an organisation has legitimate interests to process an individual’s data, unless those interests are overridden by the rights of the individual
- Consent - where the individual has given their consent to the processing of the data
- Contract - where it is necessary for the performance of a contract to which the individual is a party, or to take steps at the request of an individual prior to entering into a contract
- Legal Obligation - where it is necessary for compliance with a legal obligation to which the organisation is subject
- Protect Rights of the Data Subject - where it is necessary to protect the vital interests of an individual
- Public Interest - where it is necessary for the performance of a task carried out in the wider interests of society or in the exercise of a statutory function of the organisation.

Direct marketing is founded on a combination of different elements. Organisations collect personal data to use for insight, in order to gain a better understanding of their customers. They also create customer profiles to enable personalised direct marketing communications. Each processing activity requires a legal basis, so it can be justified under GDPR. Marketers must consider their legal basis both for profiling customers and sending the communication.

This instalment of the DMA’s GDPR guidance covers two of the legal grounds: legitimate interests and consent. We believe these two bases are the most likely to be used to justify direct marketing following the GDPR’s introduction.

The DMA’s lobbying efforts saw direct marketing enshrined in Recital 47 of the GDPR text as an example of legitimate interests. A combination of consent and legitimate interests may now be used. For example, consent to send an email to a consumer under the requirements of the EC’s Privacy and Electronic Communications Regulations (PECR) can be used alongside legitimate interests – subject to passing a legitimate interest assessment (LIA) – for any personalisation under GDPR.

Where PECR applies consent will be the only option. PECR is going to be replaced by the ePrivacy Regulation (ePR), which could potentially make all electronic marketing require an opt-in, even for marketing to employees of limited and publicly limited companies. However, the final text of the regulation is not known and it is subject to change during negotiations.

Meanwhile, compared to the existing Data Protection Act, the GDPR significantly strengthens the standard of consent. This means marketers may find that using consent as a legal basis may not work. They might prefer to use legitimate interests, where appropriate, as the legal basis for their marketing activity.

However, legitimate interests cannot be considered a “get out of jail” card. Organisations must make a compelling case as to why someone would be interested in their goods or services by carrying out robust Legitimate Interests Assessments, while also offering clear opt-outs to customers.

While the GDPR covers the processing of personal data for the purposes of direct marketing, in certain circumstances other laws may cover the use of certain channels. For example, you may need to refer to PECR, which requires marketers to ask for consent in certain contexts, such as sending an email to a consumer who isn’t an existing customer.

These amendments and extensions to existing data regulations have the potential to become a legal minefield. We aim with this guide to support you through the process of making changes to your operations to stay within the law when considering direct marketing campaigns.

Background:

The legal grounds for processing, Consent and Legitimate Interests

The two legal grounds organisations are likely to use for their direct marketing activities will be either legitimate interests or consent. Here we give our view on both, and break down what each means and under what circumstances they can be used. .

What do I need to know about legitimate interests?

Legitimate interests is a risk-based approach, where marketers must balance their interest in processing the data with any risks to the individual's privacy. Marketers must offer a clear opt-out, inform the individual of the processing activity and have a compelling case for why someone may be interested in their goods or services.

Here are the relevant passages from the GDPR text:

Under Article 6 1(f)

"...processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child."

Recital 47

"The legitimate interests of a controller, including those of a controller to which the Personal Data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."

Can I use legitimate interests?

When planning activity, take time to consider the following points:

- Do you have an existing relationship with the subject? However, it is not a requirement in all instances.
- Have you carefully weighed up the legitimate interests of the organisation with the rights of the consumer?
- Is it within the reasonable expectations of the individual?
- Has an option to unsubscribe or opt-out been provided? This is normally sufficient for your data to pass the tests set by GDPR.
- You must comply with both GDPR and the Privacy and Electronic Communications Regulations (PECR) and PECR requires you to ask for consent in some instances when using electronic channels.

What is consent?

Consent is offering people genuine choice and control over how you use their data. When consent is used properly, it helps you build trust and enhance your reputation. It must be freely given, specific, informed, and there must be an indication signifying the individual's agreement. The GDPR makes even clearer the need for an indication that is unambiguous and involves a clear affirmative action.

The definition of consent in Article 4 (11) of the GDPR is as follows:

"...any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms:

- Consent must be separate from other terms and conditions. It should not generally be a precondition of signing up to a service
- The GDPR specifically bans pre-ticked opt-in boxes
- It requires granular consent for distinct processing operations
- You must keep clear records to demonstrate consent
- The GDPR 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
- Public authorities, employers and other organisations in a position of power are likely to find it more difficult to get valid consent.

Implications for PECR

The EU is in the process of replacing the ePrivacy Directive (and therefore PECR) with a new ePR. The new ePR will not be agreed by the EU before the GDPR comes into effect on 25 May 2018. The existing PECR rules will continue to apply until the ePR is finalised and comes into effect, but with some changes to account for the GDPR. In particular, existing PECR rules will apply using the new GDPR definition of consent. The relationship between PECR and the GDPR is slightly different to that between PECR and the 1998 Act, but this does not affect the marketing rules and organisations must continue to comply with both regimes.

Which principles within the GDPR relate to personal data processing?

In addition to selecting the most appropriate legal ground for processing data, organisations must also make sure that they comply with the six principles listed in Article 5 of the GDPR. Data must be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes, and not in another manner incompatible with those purposes. However, further processing for archiving purposes in the public interest, for scientific or historical research or statistical purposes is considered to be compatible with the initial purposes
- Adequate, relevant and limited to what is needed for the purposes the data is processed
- Accurate and, where necessary, kept up to date, erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods if processed solely for archiving purposes in the public interest, or for scientific, historical research or statistical purposes as long as the rights and freedoms of individuals are protected
- Processed in a manner to protect the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
- The principle of accountability, which relates to being able to evidence your compliance with the GDPR. For example, by carrying out an LIA, to show your decision making when using legitimate interests for marketing
- Transparency. You must ensure individuals are informed about how you are going to process their personal data. Articles 13 and 14 detail all the information you must make someone aware of when you collect their personal data.

The DMA's view on legitimate interests vs consent

Many commentators have suggested that consent is the only legal ground that a marketer should rely on. The reality is it will depend on the channel being used for the marketing contact, and whether the consent requirements of PECR also apply. Some organisations have opted for consent as their preferred legal option due to its objective nature. Yet legitimate interests is an equally valid ground for marketing activity and provides marketers with more flexibility to connect with customers. Consent can give people genuine choice, but is in fact only required when no other lawful basis exists or when PECR requires it.

It's important to note that the legislation says there is no hierarchy. All legal grounds are equal and the decision to

select either consent or legitimate interests for marketing activity should be made on what is best for your customers and your organisation, so long as your intentions remain transparent. Remember, PECR requires that you ask for consent in certain contexts.

You might choose consent for some activities and legitimate interests for others. This could even happen within the same transaction. A company might decide that consent is appropriate for email marketing, but that profiling should be carried out using legitimate interests, for example. Whatever the case, let transparency be your guiding light.



Introducing: Legitimate Interests

Consent and legitimate interests hold equal validity as legal grounds to process data under the GDPR. However, the latter offers more flexibility for marketers.

Legitimate interests offers marketers a useful legal route as there are numerous instances when it applies to their activities. Opting for legitimate interests could mean avoiding the need to reconnect with people and ask for their consent.

However, you must still comply with the transparency requirements and Articles 13 and 14 detail the information you must make individuals aware of when you collect their personal data or in your first communication to them.

Recital 47 of the GDPR recognises that direct marketing may be regarded as carried out for legitimate interests. For this reason, many organisations may prefer to use legitimate interests and only ask for consent to use certain channels for marketing if they are required to do so.

Under legitimate interests, it's necessary for organisations to communicate to the data subject the type of processing that is taking place. For example, a charity informs new donors during its website registration process that their personal details will be used to send them postal direct marketing with fundraising messages. The charity offers a clear opt-out at this stage and comprehensively explains how people's personal data may be used.

Donors reasonably expect that a charity they've given money to would ask to send them fundraising communications, and the charity believes its donors may benefit from receiving such communications. Unless donors opt out, the charity can send them fundraising communications in the post, assuming that you have successfully passed an LIA and will not override an individual's rights.

Citizens' rights and Legitimate Interests

Under GDPR, people have the right to privacy and can object to their personal data being used for direct marketing.

This means that when using legitimate interests, you must also consider people's rights. You cannot use legitimate interests and override a person's rights under the GDPR if they have opted out.

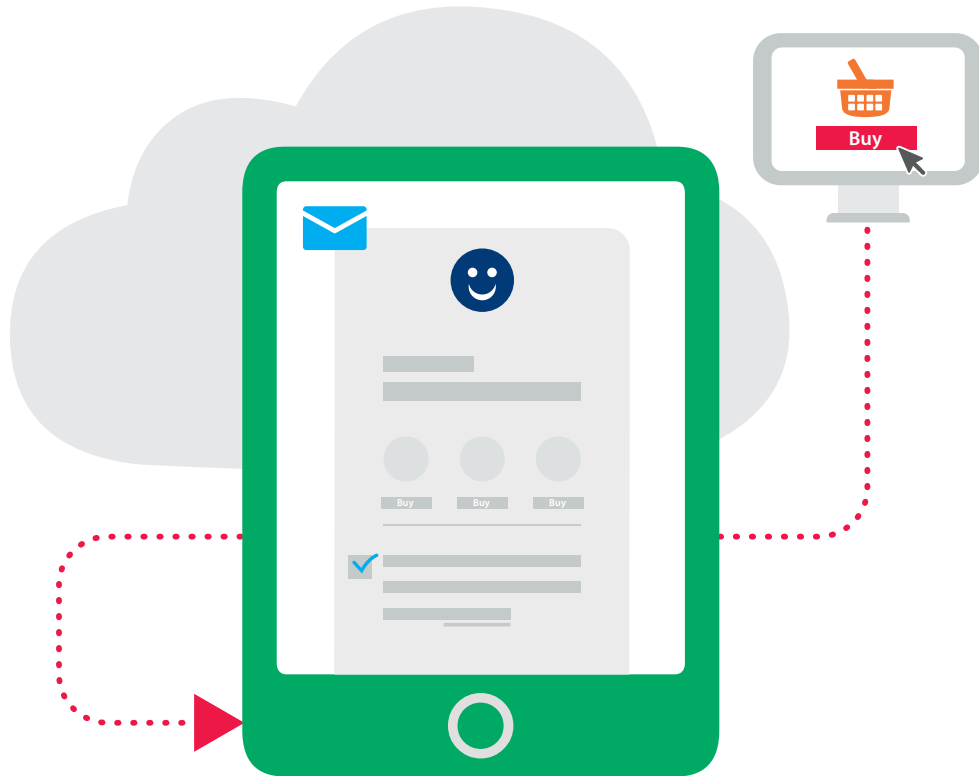
Citizens' rights must be considered when conducting an LIA to determine if you can process a person's data (see pages 14 and 15). These rights are listed below:

- The right to be informed how personal data is processed - you must inform the data subject what your legitimate interests are. This information can be included in a privacy policy linked to the data collection statement
- The right of access to their personal data – any individual can submit a personal data Subject Access Request, which the organisation must respond to in a lawful, fair and transparent manner. An example would be a job candidate asking to see data held on them after several unsuccessful applications for vacant posts at the organisation
- The right to rectification – an individual is allowed to inform any organisation of new, or changes to, their personal contact details; the organisation is obliged to amend the contact details it holds and only use them for direct marketing purposes in accordance with the law
- The right to erasure – the so-called “right to be forgotten”. An individual is entitled to ask organisations to remove information it holds on them. An example would be a newly married person who discovers their dating app profile is still live and asks for it to be taken down
- The right to restrict processing - individuals have the right to block or suppress processing of personal data if they believe it is incorrect. When processing is restricted, organisations are permitted to store the personal data, but not further process it
- The right to data portability – this allows individuals to obtain and reuse their personal data for their own purposes across different services i.e. to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way
- The right to object: an individual has the right to object to any processing that uses legitimate interests. This should be communicated at the point of data collection, perhaps via an opt-out box or link for marketing communication. For other processing, such as profiling, you might consider an email address or other mechanism
- In particular, there is an absolute right to object to direct marketing and this must be respected by organisations. Clear opt-outs should be available when personal data is collected and in all future communications
- Rights in relation to automated decision-making and profiling. An individual can object to a decision made solely on an automated basis, which has a legal or similarly significant effect. It may only happen if the decision being made is necessary for contractual reasons, or authorised by EU or UK law applicable to the controller, or based on the individual's explicit consent. Furthermore, the organisation must identify whether any processing falls under Article 22 of GDPR, give individuals information about the processing activity, allow them to challenge a decision easily and regularly check its systems are working.

When an individual's data is collected and the organisation intends to process the data for direct marketing, the organisation must make that clear to the individual. This information must be clearly displayed and separate from any other information. The person must also be told that they have the right to object if the processing is based on legitimate interests.

For example, a catalogue company sends regular offers to its customers. Or an online retailer profiles buying history to suggest likely products.

Example: existing customer soft opt-in and legitimate interests



Thank you for buying with us.

We believe that based on your purchase you would be interested in other related cloud computing solutions we offer. We will send you emails about our products and services and look forward to doing business with you again soon.

If you wish to not receive marketing from us then please click [here](#) and you will instantly be unsubscribed from our email database.

We have prepared a plain English and simple privacy policy that explains how we will use your personal data. Follow the [link](#) the find out more.

Reasonable expectations

You cannot use legitimate interests as your legal ground for marketing if the interests of the individual override your legitimate interests as an organisation. Acting outside of someone's reasonable expectations is a key test and one where an organisation might be deemed to override someone's fundamental rights.

Recital 47 says:

"At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."

This means that when an organisation collects someone's personal data they should explain that they could receive marketing. The individual should not be surprised to receive marketing, they should have been made aware that marketing would be sent to them.

An individual may not read the privacy information that an organisation makes available but it is still important to have this information ready for people. This is to ensure that individuals are informed about how their personal data will be used.

If the marketing is unexpected it is unlikely that people were aware that their personal data had been collected for marketing, therefore they cannot object to the processing. The ICO states in its legitimate interests guidance that this would result in someone losing control over the use of their personal data, which is contrary to the GDPR.

Determining whether someone would reasonably expect to receive marketing from you is easier to justify in the context of an existing relationship. For example, when sending direct marketing to a client or a consumer who has bought from you before.

If you have bought a data-set from a third party for the purpose of sending people direct marketing, then you need to check with your supplier what people were told when their personal data was collected by the third party. For example, were people told that they would receive marketing from companies within a specific sector? If they were, then you could argue that receiving marketing from similar companies was within an individual's reasonable expectations. It's important to record the checks you make so you can provide evidence of your processes.

Other factors might also affect the reasonable expectations of individuals, such as:

- how long ago you collected the data;
- the source of the data;
- the precise nature of any existing relationship with the individual and how you have used their data in the past; and
- whether you are using a new technology or processing data in a new way that individuals have not anticipated - or conversely whether there are any developments in technology or updates to services

However, it is important to remember that reasonable expectations is not the only criterion to consider when assessing whether you can use legitimate interests. You may have compelling reasons that override the lack of reasonable expectations.

For example, a sole trader builder advertises his business address on his work van. An individual working for a concrete company notes down the address and sends a direct mail piece to the builder. The legal ground for this would be legitimate interests. There is no existing relationship between the concrete company and the builder.

However, the builder reasonably expects to receive marketing because he has been advertising his company's address details in public.

Legitimate Interest Assessment (LIA)

The Data Protection Network's guidance, which the DMA helped to draft, states that an organisation should carry out an assessment to see whether it is able to validly use legitimate interests as a legal basis for marketing.

There are three stages to this assessment:

- Identify a legitimate interest
- Carry out a necessity test
- Carry out a balancing test

So, what does this mean in a marketing context?

Identify a legitimate interest

This is where an organisation contemplates the purpose of data processing activity. In marketing, this means communicating with customers or prospects to help promote or sell products or services.

At this stage, a marketer should ask why the activity is important to the organisation. For example, a computer games shop is marketing the latest release in a popular trilogy of Xbox games. Previous customers are likely to purchase after receiving this marketing as they may be interested in the new game.

Carry out a necessity test

Once you have identified legitimate interests, you must then decide whether processing activity - planned or under way - is necessary. For example, if you wanted to run direct marketing campaigns, all the processing activities you engage in for that purpose must be proven necessary.

To illustrate this point, combining personal data with data from other sources that is unnecessary for the sale of your products would be deemed excessive. Meanwhile, sharing data with a third party that would not be required to deliver the service would also be unnecessary. In either case, you may need to find another legal basis or decide to not go ahead with the campaign.

Yet the processing of personal data is an integral part of direct marketing. Without this data, direct marketing would not exist because communications could not be personalised and tailored to the target audience. In theory at least, it should therefore be relatively straightforward for a marketer to satisfy this part of the assessment. However, this cannot be assumed and must still be part of your assessment.

It is important to remember that you may have two purposes for processing personal data; profiling to establish the audience and the sending of the marketing communication. You need a legal basis for each of these and they may be different legal grounds.

Carry out a balancing test

The third, and most crucial, part of the assessment identifies the risks to an individual's personal privacy. Marketers should consider how their proposed campaign may impact this and record their findings.

Organisations may decide on several changes to the campaign as a result of the balancing test. For example, data retention periods may be introduced. By promising to delete personal data after a specific period, the risk to breaching individual privacy is reduced.

Another example would be data minimisation: only requesting personal data that is core to the marketing campaign. Requesting more personal information than is necessary increases the risk to people's privacy and is a breach of one of the principles of GDPR.

You must also consider the risk of unintended consequences, such as processing personal data in a manner allowing you to infer someone's religion, ethnicity or details about their health. This is known as special category personal data, which requires a different legal basis for processing, which cannot be processed based on legitimate interests

in this context. Article 9 of the GDPR details the cases where the processing of special categories of personal data is allowed, including if an individual has given their explicit consent.

As part of the balancing test, you will need to determine how much the individual would expect your data processing. Is it obviously relevant in the context of your relationship with them? Or would the individual be surprised if they knew what the organisation was doing with their personal data?

If people might object to the type of processing the organisation is undertaking, it is unlikely that legitimate interests will apply.

What questions should you ask?

You need to make an unbiased assessment of whether your legitimate interests tilt more towards you or whether the processing would impinge upon the individual.

Filling out the below the questionnaire will help you to decide, on balance, which course of action is appropriate.

Do the rights of the individual override the Legitimate Interests of your business?

Businesses need to make unbiased assessments of whether their Legitimate Interests tilt more towards business or customer. Respond to the below, which will help you decide:

Query	Response A	Response B	Notes
Is there an existing relationship between your business and the individual?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
If there is a relationship, is this two-way and ongoing?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Existing relationships will add to your case for using Legitimate Interests. If that relationship is two-way and ongoing, this will further enhance your case, particularly if the relationship involves recent and regular exchanges.
Would the customer expect you to process their personal data?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
Would the customer expect you use their personal information for the reason you intend to use it?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	If customers expect processing to take place then they are likely to accept that you do.
Have you told individuals clearly how and why you expect to process information?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	If you tell customers why you need to process their information, they will expect no more than this.
Can the individual object or control to the processing you propose?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	If processing only benefits your business, Legitimate Interests are led likely to be valid.
Would processing add value to the product or service your customer bought?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	If processing adds value to the customer, this makes your case for Legitimate Interests stronger.

Would processing have a negative impact on your customer's rights or cause them harm or distress?	No <input type="checkbox"/>	Yes <input type="checkbox"/>	Negative effects on your customers make Legitimate Interests less likely to be valid.
Could your business or a third party suffer negative consequences without the processing?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Negative effects from NOT processing could mean Legitimate Interests are more likely to be valid.
Would processing involve special categories of personal data?	No <input type="checkbox"/>	Yes <input type="checkbox"/>	Processing of special categories is permissible only: with explicit consent; if processing is in the public interest; or to carry out specific legal obligations. See Article 9 for more information .
Would processing undermine or limit your customer's rights?	No <input type="checkbox"/>	Yes <input type="checkbox"/>	Processing should not have a negative effect on the customer, whether that effect is now or in the future.
Is information on individuals obtained directly or indirectly	Directly	Indirectly	If information was collected directly, and if the individual was given notice of processing, then this will strengthen your case
Does the balance of power lean towards the business?	No <input type="checkbox"/>	Yes <input type="checkbox"/>	If your business is dominant, and the customer has little choice, then your case for Legitimate Interests will be weaker.
Could processing be perceived as inappropriate?	No <input type="checkbox"/>	Yes <input type="checkbox"/>	The more unusual the processing, the less likely you will be able to rely on Legitimate Interests.
Can potential risks from processing be reduced or designed out?			Whether yes or no, explain why. Look at your processes and see where there could be any impact on individuals and look at ways to reduce it. It may be that your processes are already well refined, but explain how.

In general, responses in column A are more likely to support the use of Legitimate Interests for processing, while responses in column B are likely to do the opposite.

Data Sharing and Legitimate Interests

It is possible for companies to use and share data for postal and telephone marketing (except automated telephone marketing as PECR will apply) under GDPR provided they are open about this sharing and provide an opt-out statement to give the individual a chance to object.

As with all uses of legitimate interests, a Legitimate Interest Assessment must be carried out and documented to justify the data processing and to consider the reasonable expectations of the consumer and any impact on them.

At the point of data collection you will need to be clear with the individual that their data may be used by third parties and you will need to carefully define who these third parties might be, but unlike the legal ground of consent they will not have to be individually named.

Example statement

We think you'd enjoy some of the latest products and offers by post from our trusted retail partners: companies operating in the clothing, collectables, food & wine, gardening, gadgets & entertainment, health & beauty, household goods, and home interiors categories.

If you would prefer **not** to receive these, please tick this box

To learn more about our partners and how your data may be used for marketing, see our privacy policy at www.example.org.uk

Consent as an alternative legal basis to use and share data for direct mail

Consent via an opt-in permission statement is necessary for email, SMS and automated phone calls where PECR applies but is not legally necessary for direct mail or telephone, although it is required if an individual is registered on Telephone Preference Service (TPS) or Corporate Telephone Preference Service (CTPS).

An LIA (see pages 14 and 15) must be carried out and documented to justify the data processing, considering the reasonable expectations of the consumer and any impact on them. At the point of data collection, you will need to be clear with the individual that their data may be used by third parties. You'll also need to carefully define who these third parties might be, but unlike the legal ground of consent they will not have to be individually named.



Profiling and Legitimate Interests

Organisations rely on data analytics to inform their marketing strategies. Purchasing history and other types of data are collected and examined to build intelligence within an organisation. Ultimately, this gives marketers a better picture of their customers, allowing them to personalise communications.

Under the GDPR, they must have a basis for doing so. For example, an email marketer must use consent to send emails to consumers they've had no prior interaction with, as required by PECR, but can rely on legitimate interests to process personal data of previous customers, allowing them to personalise communications, without requiring further consent.

Another example is web analytics. Legitimate interests can be used by an online retailer to monitor search data, products viewed and purchase data. Collecting this information is vital as it allows the retailer to understand its customers and prospects, and which products are popular.

This is a significant change, as web analytics information was not considered personal data under the Data Protection Act 1998 - but it is under GDPR.

Other activities that will be able to rely on legitimate interests include:

- Data hygiene - for example, using the Edited Electoral Roll to ensure home address data is correct and up to date. However, you would have to consider whether an individual's rights would override this in an LIA
- Data deduplication (de-dupe) - for example, it is possible that an individual customer might appear in multiple segments, especially if you are sending a campaign to groups defined by different criteria. Duplicate copies of the same customer should be removed
- Credit checks - for example, a bank is required to process personal data to be able to assess whether it can sell someone a particular product. This can be done under the auspices of legitimate interests. However, this may be justified under contract as using legitimate interests means you need to provide an opt-out, which you may not want to do in this situation.

PECR and Legitimate Interests

Compliance with PECR is required when marketing to consumers via email and SMS, whereas in telemarketing (except automated calls), PECR allows for an opt-out approach, provided the data is screened against TPS and where applicable CTPS.

To rely on legitimate interests for digital marketing, organisations must ensure the following:

- The email address and SMS number were collected during the sale of goods or services (although the person does not need to have completed the purchase)
- The marketing communications must be about similar goods or services to those purchased or enquired about
- **Most importantly, someone must be given an opportunity to object to electronic marketing, each time they are sent a marketing message, as well as at the time the data was collected.**

Business-to-business (B2B) marketing (defined as limited, public limited companies and public bodies such as schools and hospitals) are not covered under PECR, which means that you do not need prior consent in order to send emails or SMS communications. Marketers may therefore be able to use legitimate interests for B2B campaigns.

Example: Email marketing and legitimate interests

The PECR allows marketing to be sent to existing customers without asking for their consent, which would give organisations legal grounds under legitimate interests according to the GDPR.

However, you must also comply with all the existing customer soft opt-in requirements in PECR.

An online retailer has a large amount of email addresses for its previous customers. The online retailer is allowed to market similar products to existing customers based on their previous purchase(s).

The retailer must abide by all of the other requirements of PECR's existing customer soft opt-in.

On this basis, the retailer can continue to send marketing emails to existing customers without having to ask for their consent to do so. This example does not just apply to email, but also to SMS and telephone marketing.


However, they must comply with all the other requirements of the existing customer soft opt-in. You can read more about PECR on the ICO website: <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>

PECR specifically addresses electronic marketing channels, rather than offline channels such as direct mail. This means consent is not required for direct mail or telephone marketing (unless it is for automated calls or to individuals registered with TPS or CTPS).

It is worth keeping in mind that PECR is subject to change. It is informed by the ePrivacy Directive, which is being reviewed by the EU and will become the ePrivacy Regulation in the future. This could potentially impact the soft opt-in, however the final text has not yet been agreed. The latest version of the ePrivacy Regulation retains the existing customer soft opt-in.

The chart below summarises where legitimate interests is appropriate:

	Marketing method	GDPR legal basis	
		Legitimate interest	Consent
PECR applies	Emails/text messages to individuals - without 'soft opt-in'		
	Emails/text messages to individuals - obtained using 'soft opt-in'		
	Automated phone calls		
	'Live' phone calls to TPS/CPTS registered numbers		
Non-PECR	'Live' phone calls where there is no TPS/CPTS registration or objection		
	Post/direct mail to business contacts		
	Post/direct mail to consumers		
	Emails/text messages to business contacts		

 Indicates correct legal ground

Introducing: Consent

Consent in marketing

Under the GDPR, consent means actively agreeing to the stated processing, whether in writing, verbally or electronically. Examples include:

- Ticking a box when visiting a website
- Choosing technical settings for cookies on your internet browser such as Microsoft Internet Explorer, Firefox, etc.
- Any other statement or conduct which indicates acceptance, e.g.:

“By submitting your email address in the box below, you agree that Organisation A may send you special offers about their products and services by email in the future.”

The GDPR text states that consent does not include:

- Silence
- Pre-ticked boxes
- Inactivity

By taking positive action, a consumer should be in no doubt as to whether or not they will be receiving marketing from your organisation, what sort of marketing is involved and the channels that will be used to communicate with them.

People must be presented with a genuine choice about whether they agree that their personal data can be used for marketing. Being clear and transparent is key. Tailor the language in your consent statement to your target audience and always ensure it is clear, and easy to understand.

What do I need to do now?

You will need to review your consent mechanisms to make sure they meet the GDPR requirements. The key new points are as follows:

- **Unbundled:** consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service
- **Unbundled:** consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service
- **Granular:** give granular options to consent separately to different types of processing wherever appropriate, for example separate tick boxes for each marketing channel
- **Named:** name your organisation and any third parties that will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR
- **Documented:** keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented
- **Easy to withdraw:** tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place
- **No imbalance in the relationship:** consent will not be freely given if there is imbalance in the relationship between the individual and the controller. This will make consent particularly difficult for public authorities and for employers, who should look for an alternative legal basis.

What counts as valid consent for marketing?

The definition of consent in the GDPR builds on the definition in the 1995 Data Protection Directive, which states: "...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."

The GDPR definition retains the key elements that comprised the 1995 Directive's version, but several points have been fortified: "...any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Should I include the opportunity to withdraw consent?

Make it clear that someone can withdraw their consent and include details of how to do so. Consent should be as easy to take away as it is to give.

If consent is given via a tick box online, then a very similar and easy process to withdraw it must be in place. Organisations must not put obstacles in the way of somebody who wants to remove their consent.

For example, an email marketer sending a customer regular emails should not make that person send a piece of mail or make a phone call in order to revoke consent. The person should be able to remove their consent easily over email.

What is specific and informed consent?

An organisation must give someone the following information for consent to be specific and informed:

- The identity of the organisation - the data subject must be made aware of the organisation asking for their consent
- The purposes of the processing - why does your organisation need personal data from somebody? Make your reasons for requesting a piece of personal data very clear
- When collecting personal data for marketing purposes, the consent for the marketing should be separate from other requests to collect personal data. For example, requests for personal data for marketing, and for other terms and conditions, should be separate
- Name your organisation and any third parties that will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR
- If you are undertaking any processing activities for marketing, apart from those that require a marketing communication to be sent, you must inform the data subject, giving granular options for the different types of data processing. These can be detailed in a privacy notice, and include:
 - Data and behavioural analysis
 - Profiling
 - Segmentation
 - Social media monitoring
 - Combining data from third parties
 - Any other processing that is being undertaken for the purposes of direct marketing.

As a minimum, individuals must be informed about the types of processing being undertaken. If the specific processing activity is not brought to their attention, consent will not be informed, so it won't be valid.

Will I need to review consent over time?

Once you've gained consent you must keep it under review. People have only given consent for the processing specifically brought to their attention in any statement made during the data collection process. If your organisation wishes to change any of the processing activity, or repurpose the data, you must fully inform the individual and obtain further consent.

What is unambiguous indication?

The GDPR's Recital 32 fleshes out the meaning of clear affirmative action:

"Consent should be given by a clear affirmative act... such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting a website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

The key takeaway here is that consent as part of GDPR requires an opt-in. There is no such thing as opt-out consent using the GDPR definition.

However, the definition of affirmative action does still leave room for some forms of implied consent, especially in informal situations. For example, a marketing services supplier has a stand at a marketing exhibition featuring a bowl for business cards in which visitors can leave their details to find out more about products and services. Alternatively, someone has their exhibition badge scanned to capture their details.

The scenarios outlined are affirmative acts that clearly indicate someone agreeing to their personal data being used for marketing about the products and services advertised at the exhibition. You would still need to meet the requirements of being specific and informative to the individual, and you'd also need to consider how to prove valid consent if challenged.

What are the rights of an individual under consent?

Individuals will have more rights if an organisation uses consent as the legal ground for processing personal information for direct marketing purposes. These rights make it more difficult for organisations to obtain consent.

If you plan to use consent as your legal ground for marketing, GDPR details several additional requirements:

- Article 7 sets out various conditions for consent with specific provisions on:
 - Keeping records of consent
 - Making consent requests clear and prominent
 - The right to withdraw consent
 - Not making consent a condition of a contract, unless it is a fundamental part of the service.
- There are special rules on children's consent for both online services (with a child defined as a person under 13 years of age under UK law), and for scientific and research purposes
- People have a right not to be subject to a decision based solely upon automated decision-making, unless they have given their explicit consent.

When should I ask for consent?

If you have chosen consent as the most appropriate legal basis for processing personal data for direct marketing, you must obtain consent **before** any processing of data happens. Therefore, you must ask for consent at the point of data collection.

You must also ask for explicit consent when processing special categories of personal data, unless another Article 9 condition is more appropriate. Included in the GDPR definition of special categories of personal data are the following:

- Racial or ethnic origin
- Political opinion or affiliation
- Religious or philosophical belief
- Trade union membership
- Health
- Sex life or orientation
- Genetic data
- Biometric data used to identify a person.

What is the “standard of consent”

The standard of consent has now been significantly increased since its initial outline in the 1995 Data Protection Directive. This strengthened definition will have far-reaching consequences if not interpreted accurately. In order to obtain consent under the new standard, it must meet the following requirements:

- There must be a clear indication of the subject’s wishes
- They must take an affirmative action
- Consent must be separate from other terms and conditions
- You must seek granular consent for different processing methods
- You must maintain evidence to demonstrate consent
- Consent should be a real choice, so only offer it if there is genuine choice available to someone.

Consent



An objective legal ground. Marketers must ask someone for their permission to process their personal data. This could be by ticking a box online or answering yes over the telephone.

Consent must be freely given, informed, unambiguous and given by a clear affirmative action.

Consent must be...



 Clear indication of the data subjects wishes	 They must take an affirmative action
 Consent must be separate from other terms and conditions	 You should seek a separate consent for different processing
 Maintain evidence to demonstrate consent	 Consent should be a real choice so only offer it if there is genuine choice available to someone

If you already have consent from your customers to market to them, then in order to continue that relationship you will need to ensure that it meets the GDPR's consent requirements.

What's the difference?

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



DP
1995



GDPR
2016

any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

The key elements that comprise consent are still there but a number of aspects have been strengthened.

Consent does not include...

-  Pre-ticked boxes
-  Opt-out or implied consent is not a valid form of consent
-  Silence or inactivity is not a valid form of consent
-  The privacy policy must not be hidden and you mustn't use ambiguous language



The ICO say in their guidance that:

"You are also likely to need consent under ePrivacy laws for most marketing calls or messages, website cookies or other online tracking methods, or to install apps or other software on people's devices."

There is going to be a new ePrivacy Regulation.

How long does consent last?

There is no set period for the lifetime of consent under the GDPR.

How long consent lasts will depend upon the individual context, so organisations must determine the duration themselves. This also means justifying, when challenged, why it has chosen the data retention period. This aspect must be documented and form part of an organisation's records of processing activities.

For example, if a customer gave consent to receive messages about healthy eating during summer, consent would be expected to expire once autumn arrived.

However, some products, such as car or home insurance, renew annually, meaning it might be appropriate for consent to last a year.

The DMA advises its members to adhere to these minimum standards on the lifetime of consent:

- **For third-party data:** telephone, email, SMS; the maximum time that consent can remain valid is six months after initial collection or any other positive contact, as defined below
- **For third-party postal marketing:** the maximum time consent can remain valid is 24 months after initial collection or any other positive contact, as defined below
- **For all first-party data:** telephone, email, SMS and post; the maximum time that consent can remain valid is 24 months after initial collection or any other positive contact, as defined below.

The timeframes run from either the initial collection or further positive contact with the customer.

Initial collection

This is defined as the moment an organisation obtains consent from someone to process their personal data for direct marketing. The organisation must maintain a record of the consent and an audit trail for evidence.

A positive contact

You must have proof that someone is continuing to engage with your organisation after they've given their consent.

For example, they've bought recommended products from an organisation, or clicked through from a marketing email to browse a website. These instances demonstrate an ongoing relationship between an individual and the organisation.

The data controller cannot rely on the absence of an action by the data subject as an indication of consent. There must be a dialogue, defined as a two-way communication via any channel, in which both parties exchange ideas, questions and answers.

Why do I need to record consent?

One of the key changes in the GDPR is the accountability principle. This relates to the recording of consent.

The onus is on organisations to be able to demonstrate their compliance with the law under the accountability principle. You should be able to show someone that they consented to receiving marketing from you, by providing them with a clear audit trail from the time and date of consent.

The inability to show a valid audit trail to someone asking for proof of their consent is considered a breach of the GDPR. In order to have a valid audit trail you must maintain records that demonstrate the following:

- **Who consented:** record their name, or other identifier such as username
- **When they consented:** a copy of a dated document, or online records that include a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation

- What they were told at the time - a copy of the data capture form that was used, and the privacy policy that the person agreed to when they gave their consent, should be attached to the record. Version numbers and dates should match the date of consent. If consent was given to a member of your contact centre staff, a copy of the telephone script used should also be saved
- How they consented - keep a copy of the written statement or online form someone used to give their consent for marketing. In an online context, it will be easier to include the data given as well as a timestamp to link it to the data capture form that was used
- Withdrawing consent - if someone does withdraw their consent, a record of the date and time should be kept, too.

Consent requirements in practice

The examples below illustrate specific elements of consent, and do not necessarily indicate all of the requirements of a consent statement. PECR also applies in some of the examples below.

Unbundled / Separate

The individual's consent to direct marketing must be separate from other terms and conditions.

You cannot make people give you consent as a condition of a service (as it would not be freely given). For example, the following statement would not be allowed according to GDPR:

Download Our Latest White Paper

To download your free white paper, please provide your name and email address. You will be sent to the download page once you submit your details. By providing your details, you will also be signing up for our regular newsletter and marketing emails. Thanks!

Example (business to consumer): Sainsbury's

Here's a great example of consent to direct marketing being separated from other terms and conditions. However, Sainsbury's should give people control over which channel they consent to. For example, by using a separate tick box for each marketing channel. This is how Sainsbury's tackled the issue on its website:

The screenshot shows the Sainsbury's website registration form. It is divided into two distinct sections for consent:

- Terms and conditions:** A section with a heading, explanatory text, and a single checkbox labeled "I agree to the terms and conditions."
- Contact permission:** A section with a heading, explanatory text, and two radio button options: "Yes please, I'd like to hear about offers and services." and "No thanks, I don't want to hear about offers and services."

A "Register" button is located at the bottom right of the form.

Example (business to business): Data Protection Network

Here's another example of how unbundled consent can work. It's vital that different aspects are kept separate:

The screenshot shows the Data Protection Network (DPN) website registration form. It is divided into two distinct sections for consent:

- Terms & Conditions:** A section with a heading, explanatory text, and a checkbox labeled "I agree to the Terms & Conditions".
- Join our mailing list:** A section with a heading, explanatory text, and a checkbox labeled "Data Protection Network".

A "Submit and Confirm" button is located at the bottom of the form.

Example (business to consumer): Age UK

The charity splits marketing consent into checkboxes for email, telephone, text message and post when a donor is filling in an online form to give money:

Keep in touch with us

Please tick the boxes below to tell us all the ways you would prefer to hear from us:

- Yes please, I would like to receive communications by email
- Yes please, I would like to receive communications by telephone
- Yes please, I would like to receive communications by mobile (text message)

Example (business to consumer): HomeServe

HomeServe has already taken the new requirements for consent into consideration. What used to be pre-ticked boxes for contact preferences have been replaced by unticked boxes for each relevant channel, with an explanation of how the company handles the data it receives.

HomeServe's old consent statement will not be allowed under the GDPR:

Marketing preferences


HomeServe will use your information to arrange and administer your insurance policy, for handling any claims made under the policy and for keeping you up to date with any changes to your policy or account. It may also use the information for training, quality control, research and statistical analysis. If you would like further details on how HomeServe uses your information, please see the privacy policy.

We would love to keep you up to date on offers, news and events that we think you'll find interesting. We respect your privacy and promise not to inundate you with marketing messages, however, **if you prefer NOT to be contacted please untick the following boxes.**

By Email By Phone By Post By SMS

[Next](#)

Customers are now required to tick a box if they wish to be contacted again. It's important to note that in the new example, no tick means no consent:

Plumbing & Drainage Plus Reply Form Product Ref: <mailcode> 

We (HomeServe Membership Ltd) would like to get in touch from time to time about offers and services that we think you'll love.

Our pledge to you:

- We promise we won't inundate you
- We'll keep it relevant
- We'll always keep your data safe
- We'll never share your details with anyone else
- You can change your mind whenever you like

Yes to post Yes to Email
 Yes to telephone Yes to SMS

Three simple ways to reply. Call on
0800 <XXX XXXX>
 quoting <mailcode>

£1
month
INTRODUCTORY PRICE
IN THE FIRST YEAR

Visit offer.homeserve.com/<mailcode>
 or complete and return this Reply Form

Lines open weekdays: 8am - 8pm, Sat: 8am - 4pm and Sun: 10am - 4pm.
 Calls may be recorded for quality control and training purposes.

Declaration

By completing and returning this Reply Form I agree to purchase Plumbing & Drainage Plus and enter into a contract with Aviva Insurance Limited to provide the insurance and a separate contract with HomeServe Membership Ltd to arrange and administer the insurance. I acknowledge that the key information about this insurance is set out in the enclosed information leaflets. I confirm I am eligible for this policy and that it meets my needs as a homeowner requiring assistance in the event of a plumbing, drainage or water supply pipe problem or emergency at my domestic property.

Example (active opt-in): RSPB

The RSPB requires donors to actively choose whether or not they want to be contacted. Customers cannot complete registration until a “Yes” or “No” box is ticked for each channel:

If you're happy for the RSPB and RSPB Shop to keep in touch, please let us know how you would like to hear from us:

I would like to be contacted by (please tick “Yes” or “No” in each instance):

Post	Phone	Email	Text
<input checked="" type="checkbox"/> Yes please <input type="checkbox"/> No thanks	<input checked="" type="checkbox"/> Yes please <input type="checkbox"/> No thanks	<input checked="" type="checkbox"/> Yes please <input type="checkbox"/> No thanks	<input checked="" type="checkbox"/> Yes please <input type="checkbox"/> No thanks

Example (named organisations): Nectar

If a first-party organisation is passing personal information on to third parties to carry out their own direct marketing activities, those third parties must be specifically named, rather than just the sector they operate in.

Nectar Sponsors	
Trading Names	Full Corporate Name
Alton Towers Resort Theme park, Chessington World of Adventures, SEA LIFE centres & Sanctuaries, Madame Tussauds London, LEGOLAND @ Windsor, THORPE PARK, Chessington World of Adventures & Zoo, Warwick Castle (Parks Seasonal)	Merlin Entertainments Group
American Express	American Express Services Europe Ltd.
Argos	Argos Ltd.
BOC	BOC Limited
BP	BP Oil UK Ltd.

For example:

Tick this box to hear from us - **ABC Airways** - about offers on flights to the US and Canada
 Tick this box if you would like to hear from **XYZ Hotels** about offers it has in our destination cities

You need to be careful about how this information is organised and displayed, ensuring the consumer is able to understand it while not disrupting their experience.

It's important to remember that outsourced service providers, such as an email broadcaster sending out first-party emails on behalf of an organisation, **are not** third parties.

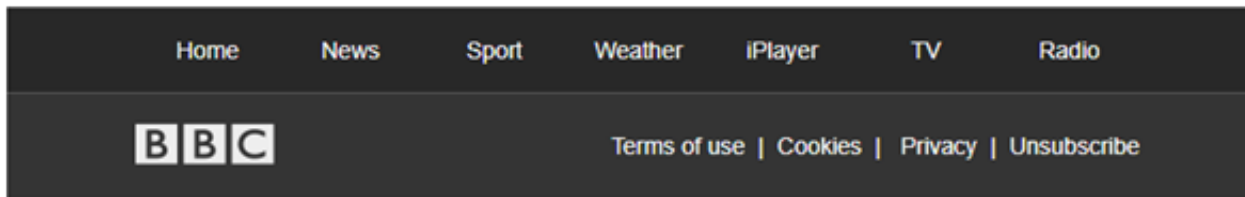
Easy to withdraw

Individuals must be able to withdraw their consent as easily as they gave it. This is also a requirement of PECR.

You must also make sure people know that they can withdraw their consent and give them straightforward ways to do so.

Example (business to consumer): BBC

The broadcaster offers newsletter subscribers the option to unsubscribe in each email they send. All it takes is one click:



To stop receiving BBC newsletters [click here to unsubscribe](#).

Refreshing consent**Using consumer data captured prior to the GDPR coming in to force:**

The GDPR does not necessarily require you to re-permission all your customers. It depends on the circumstances under which you initially obtained the data, and whether this meets the standards of the GDPR.

In some instances, consent already collected under the 1998 Data Protection Act and PECR will not be valid under the GDPR. This means marketers must reconnect with people to obtain fresh consent that reaches the new, robust GDPR standard. This process is referred to as “refreshing”.

Refreshing consent for people on your database can be a risky process, as once you’ve asked for consent and you don’t hear back, the individual is effectively saying no. People who say no or do not reply can no longer be contacted after May 25th, 2018.

Consider your approach to reconnecting with people carefully. Trial different approaches in smaller batches in order to maximise the number of people that give you their consent for marketing.

In several recent cases policed by the ICO, organisations failed to take opt-outs and unsubscribers into account, and were fined. The ICO issued civil monetary penalty notices because it upheld that these companies attempted to upgrade the consent of people who had opted out.

Meanwhile, one case was processed following a single complaint, which is illustrative of how serious the ICO will treat such cases.

Re-permissioning is not needed if your current consents meet the standards laid down in the GDPR. This means they must be “...specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn”. If they do not, you will need to “... seek fresh GDPR-compliant consent, or find an alternative to consent”. If you are not satisfied your current consents meet this standard, you will have to re-permission all those records.

Once an organisation has obtained fresh consent that meets the standards required by GDPR, it is free to process that data for the purposes of direct marketing. Remember, though, that in many instances marketers may prefer to rely on legitimate interests as a legal basis for processing personal data for marketing purposes. Legitimate interests offers more flexibility for marketers than consent but do not forget to ask for consent where PECR applies.

Refreshing Consent

Case study (business to consumer): RNLI and re-permissioning

The lifeboat charity produced work that made waves by involving its audience's emotions, rallying people to their cause and driving opt-ins as a result. The RNLI made a pledge never to contact supporters again unless given renewed permission. The reason for opting in had to be immediate and powerful.

The strategic thinking behind the campaign flowed as follows:

- Consent is based on trust, which the charity sector was devoid of following recent marketing scandals. The RNLI aimed to unpick the real drivers behind consent and provide the public with a powerful incentive: if we can't reach you, we can't reach others
- Research revealed that only 6% of people would renew permissions; the RNLI needed 22%
- There was also a "privacy paradox" that people demand rational information but make emotional decisions.

People may worry about giving their email to a retailer while sharing their most intimate moments on Facebook. The charity floated the idea of stripping away marketing jargon to encourage sign-ups. The consequence of not opting in was rooted in its human cost: fewer donations, fewer lives saved.

The creative thinking behind the campaign centred around these insights:

- The RNLI receives hundreds of distress calls every day. The creative journey started by adopting this sense of urgency
- "Communication saves lives" was the call to arms, driven home by three distinct waves over a 12-month period. The first execution went local and personal with a direct plea from supporters' nearest lifeboat station and the charity's chief executive
- The second was a national call, made using radio, broadsheet print ads and targeted Facebook videos, supported by a digital hub. This featured a compelling image of survivors of previous rescues, stood in the shape of a "tick", whose stories were retold in an emotive series of online films using real-life rescue footage
- The RNLI's final push reached out to the wider supporter community to create "a movement of the advocated" – arming supporters with an emoji tick and Facebook header they could use to update their page after opting in.



Lifeboats COMMUNICATION SAVES LIVES

HE BRAVES WAVES HIGHER THAN HOUSES TO SAVE LIVES

ALL WE NEED FROM YOU IS ONE TICK

One tick gives us permission to stay in touch with you. One tick tells us there are RNLI supporters we can count on. And your one tick means we can continue saving lives together.

Thousands of supporters have already ticked – will you?

VISIT RNLI.ORG/TICKTODAY OR CALL 0300 300 9918

Royal National Lifeboat Institution (RNLI), a charity registered in England and Wales (2099083) and Scotland (SC037701). Registered charity number 20003356 in the Republic of Ireland.

Photo: RNLI/Chris Munn

Case study (business to consumer): RSPCA and consent

The animal welfare organisation started putting plans in place for the GDPR by setting up a consent task force in November 2016. Ultimately, the charity decided to implement a consent led approach for all direct marketing activity based on channel-level opt-in (email, post, SMS and phone). Supporters will also be able to refresh their preferences during a second stage of communication.

The task force included a specially appointed data protection expert. The framework for reviewing the RSPCA's entire consent contact strategy – which had been in place for new supporters from 2016 – featured:

- Reviewing existing arrangements
- Conducting a survey into supporter requirements and expectations
- Testing consent wording to ensure clarity
- Re-examining consent capture and storage
- Developing a new consent database
- Updating its privacy policy
- Rolling out a programme to reconfirm consent.

Each element was treated as an individual work stream. This thorough and structured approach resulted in several key strategies to future-proof the RSPCA's approach to consent and to allow for flexibility to adapt to the evolving legislative environment.

The supporter research revealed that donors didn't feel existing levels of communication were excessive; in fact, they said they'd be happy to receive a broader range. Conversely, supporters claimed that a greater level of opt-in options would be confusing, possibly leading to more people appearing unwilling to receive communications based on their stated preferences. With this feedback in mind, along with legal counsel and ICO guidance, the following supporter consent statement was produced, with a view to it being clear, informative and unambiguous:

Marketing Preferences

We'd love to keep you updated about our work. This may include supporter magazines and updates, appeals and fundraising activities, volunteering and membership opportunities, shop products and other services. Your details will only be used by the RSPCA – we'll **never** share your information with other organisations to use for their own marketing purposes. Please tell us how you would like to hear from us (by ticking these boxes you confirm you're 18 or over).

Post Phone Email SMS

Should you wish to change your communication preferences please email: supportercare@rspca.org.uk or call our Supporter Services Team on: 0300 123 0346. Information about how we use your personal data is set out in our privacy notice, published at: www.rspca.org.uk/privacy

RSPCA comprises both the charity and our trading company, RSPCA Trading Limited (company number 1072608) (RTL), a wholly owned subsidiary, which runs our online shop. (SF_1.0)

Another major development proposed by the task force was the creation of a single consent database (including the bulk of fundraising data) to consolidate, store and manage all consent information. Other databases holding supporter consent information for specific purposes would be made more organised and consistent. This ensures immediate compliance with GDPR while the charity migrates all consent information to a single database throughout 2018.

Additionally, enabling adequate consent also requires scrutiny of data processing activity for direct marketing, with more detailed and clearer descriptions now included in the RSPCA's privacy policy. Alongside this, other legal bases for processing have also been assessed.

A three-stage programme to reconfirm consent kicked off in late 2017 and was planned to run until summer 2018. The consent capture initiative is focussed on reconnecting with supporters and giving them confidence to continue their relationship with the RSPCA. When signing up, the supporter views a catch-all statement for each channel; at a later stage, they'll have the opportunity to tailor preferences and provide more detailed consent per channel.



The charity says that the explicit new consent statement has improved supporter understanding of what they are opting in to receive, as well as how they could change preferences at a later date. Opt-in rates have increased compared to communications featuring the previous version.

The first phase of activity in November 2017 resulted in 10% of recipients completing and submitting the consent form. The C5 version of the mailing garnered an overall response rate of 21.5%; with a 43% response rate from our most engaged audiences.

Overall, the charity feels its approach to consent fully embraces the spirit of the new legislation, reflects supporter expectations and has adequate evidence to back it up. And, vitally, it's as easy to opt out as it is to opt in. This philosophy will engender greater levels of trust between the supporter and the charity.



Vulnerable consumers and children

Consent and vulnerable consumers

Under the GDPR, organisations can assume that all adults have the mental capacity to give consent.

However, if the organisation is aware it's dealing with vulnerable people, it may need to simplify consent statements even further to ensure recipients can understand them and give valid consent.

For more information on how to communicate effectively with people who require extra care and attention, download the DMA's guidelines on dealing with vulnerable consumers: <https://dma.org.uk/article/white-paper-guidelines-for-call-centres-dealing-with-vulnerable-consumers>

Consent and children

The GDPR allows individual EU countries to decide at what age between 13 and 16 to set the age of consent for data processing. The UK Government opted to maintain the age at 13.



Using Consent and Legitimate Interests Together

Direct marketing entails many different types of data processing. For every process, a legal basis is required in order to process personal data. An organisation must have an appropriate legal basis before processing activities take place. As discussed throughout this guidance document, that is likely to be consent or legitimate interests for direct marketing.

In many situations, a combination of the two legal grounds is best: legitimate interests may be used to justify one type of data processing for direct marketing and consent for another.

An organisation may have consent to send a marketing communication, but must assess whether it has a legal basis for all of the profiling and targeting activity that goes on behind the scenes. Without profiling and targeting, organisations would be unable to send intelligent and customer-centric direct marketing. Profiling is an integral part of direct marketing and it requires a legal basis under GDPR.

It is unlikely that a marketer would seek to use consent for the profiling element of the marketing campaign, as legitimate interests offers greater flexibility. Consent may be required if the profiling can infer someone's political affiliation, for example, as this is special category data, which would require consent in this context. However, where this is not the case legitimate interests will likely be the preferred legal basis.

For example, a mobile marketer wants to contact consumers and needs their consent to send them marketing via SMS. It collects consent from people, enabling it to send those individuals messages. This is a requirement of PECR. However, the SMS marketer also needs a legal basis to analyse the personal data so direct marketing can be created and properly targeted. This could be justified under legitimate interests. Therefore, when asking for consent, the SMS marketer also explains they will use people's personal data for analytics and targeting, so it can create personalised direct marketing, but offer an opportunity to opt out of this processing.



Conclusion

Of all six legal grounds for processing data for marketing purposes, consent and legitimate interests are the most relevant.

Marketers should check carefully that consent is the appropriate legal ground before deciding to ask for it. Once consent is sought, unless someone actively agrees, they cannot be contacted again.

A common misconception about the GDPR, and the existing PECR, is that the only option available to marketers is consent. After all, the ICO says consent is required when no other legal basis can be applied. However, it is only mandated in certain circumstances. Where consent is not legally required, legitimate interests is just as valid a legal basis.

Because of its flexibility, legitimate interests should be considered a viable option, if not a preferred option, by marketers. However, it still requires organisations to be clear from the outset about how they intend to process the personal data and offer a very clear opt-out. The DMA considers opt-out the most vital part of legitimate interests.

Ensure your organisation serves people an information notice informing them of the legal basis you have chosen for your processing.

The GDPR significantly raises the bar in terms of marketers' accountability, to not just comply but evidence that compliance. This is why whichever legal basis you decide to use, documenting your processes and recording your outcomes is vital.

This mirrors the DMA's own code, and our commitment to respecting privacy and transparency in marketing. We stress that:

- Marketers must act in accordance with customer expectations
- Those customers must have a clear understanding of the value exchange when sharing personal information
- Companies must be upfront and clear about data collection and how they intend to use the information
- Companies must avoid intrusive, excessive marketing
- Companies must not target vulnerable customers irresponsibly.



Further reading: ICO Guidance

The ICO has published draft GDPR Consent Guidance: <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>

The ICO's final GDPR guidance for legitimate interest is available online.

Legitimate interest guidance: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>

While, the final version of consent guidance has not been published yet, the ICO have confirmed that it will be largely unchanged from the draft version published in March 2017. The ICO also published a consultation summary in October 2017

Draft consent guidance: <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>

Consent consultation summary: <https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2172546/summary-of-responses-gdpr-consent-20171018.pdf>

As the ICO points out, organisations don't always need consent, and other lawful bases such as legitimate interests may be more appropriate.

For the latest on the timetable for GDPR Guidance: <https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/>

GDPR Glossary

The GDPR uses terminology that marketers may not be familiar with. In order to provide clarity, the DMA has translated these legal terms so that marketing teams – those implementing the changes GDPR requires – and not just legal teams can fully understand the language used.

Anonymous data: The process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.

Consent: “means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Controller: The organisation or individual that determines how the personal data is processed.

Legitimate interests: A legal ground that can be used to process personal data for direct marketing. As well as providing the right for individuals to object to the processing of personal data based on LI, the GDPR sets out strict criteria for organisations that seek to rely on it. These include establishing that the processing is necessary and that a balancing test has been conducted.

Personal data: Any information that can be used to identify a person is personal data. For example, names and email addresses are personal data because they reveal someone’s identity. The GDPR expands the definition of personal data to include IP addresses and online identifiers such as cookies.

Personal data breach: A breach of security that means unauthorised individuals or groups are able to access personal data. This could be the result of hacking by outside groups or because an employee made a mistake.

Data protection by design: A concept introduced by Information and Privacy Commissioner of Ontario Dr Ann Cavoukian in the 1990s. It was globally recognised in 2010 by the assembly of International Data Protection and Privacy Commissioners as an essential component of fundamental privacy protection. It has been adopted in GDPR, whereby an organisation considers what impact a particular campaign, product, system or process may have on privacy from the start. In a marketing context, this means identifying a campaign’s risks for privacy and/or data protection, recording and taking appropriate steps to mitigate them - considering privacy from the start and not as an afterthought.

Data protection by default: Similar to data protection by design, this phrase refers to privacy settings on goods or services. For example, when a phone app goes to market it should have its default privacy settings on the highest possible level. The user could then decide to lower the privacy settings.

Processing: Any operation conducted on personal data, which may include collecting, recording, storing, structuring, organising, transmission or dissemination of personal data.

Processor: The organisation that only processes personal data according to the instruction of the data controller. For example, an email services organisation only processes personal data in line with what its client discloses, making the email company a data processor.

Profiling: Any type of automated processing of personal data that evaluates the characteristics of someone to decide. Marketing segmentation or targeting is a type of profiling.

Pseudonymisation: A method of making personal data no longer personal, meaning someone could not be identified from the data. It is a process that reduces the privacy risks for people as they can no longer be identified.

Special categories of personal data: Criteria of personal data that are subject to stricter requirements because of their sensitive nature. GDPR lists the following as special categories of personal data: "... racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Supervisory authority: An independent public authority responsible for enforcing GDPR. The ICO is the supervisory authority in the UK.

Third party: Any organisation or individual that is not the data controller or processor that is authorised by either the controller or processor to process personal data. For example, if an organisation sold personal data to another organisation, the organisation purchasing the personal data would be classed as a third party.

About the DMA

A DMA membership will grow your business. Our network of more than 1,000 UK companies is privy to research, free legal advice, political lobbying and industry guidance. Our members connect at regular events that inspire creativity, innovation, responsible marketing and more. Most of them are free.

A DMA membership is a badge of accreditation. We give the industry best practice guidelines, legal updates and a code that puts the customer at the heart. We represent a data-driven industry that's leading the business sector in creativity and innovation.

One-to-one-to-millions marketing attracts the brightest minds; individuals who will shape the future. By sharing our knowledge, together, we'll make it vibrant.

Published by The Direct Marketing Association (UK) Ltd Copyright © Direct Marketing Association. All rights reserved.

www.dma.org.uk



About our partners

The Data Protection Network is an online community dedicated to providing expert opinion, quality resources, informative events and learning materials, to both experts and non-experts in the field of Data Protection and Privacy.

dpnetwork.org.uk



ISBA represents the leading UK advertisers. We champion the needs of marketers through advocacy and offer our members thought leadership, consultancy, a programme of capability and networking.

We influence necessary change, speaking with one voice to all stakeholders including agencies, regulators, platform owners and government.

Our members represent over 3000 brands across a range of sectors. Over a hundred members are represented on our Data Action Group, which provides discussion, events and guidance on GDPR.

ISBA is a member of the Advertising Association and represents advertisers on the Committee of Advertising Practice and the Broadcast Committee of Advertising Practice, sister organisations of the Advertising Standards Association, which are responsible for writing the Advertising Codes.

We are also members of the World Federation of Advertisers. We are able to use our leadership role in such bodies to set and promote high industry standards as well as a robust self-regulatory regime.

isba.org.uk





Copyright and disclaimer

GDPR for Marketers: Consent and Legitimate Interests 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 *GDPR for Marketers: Consent and Legitimate Interests*, 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 to be correct at January 2018. All corrections should be sent to the DMA for future editions.