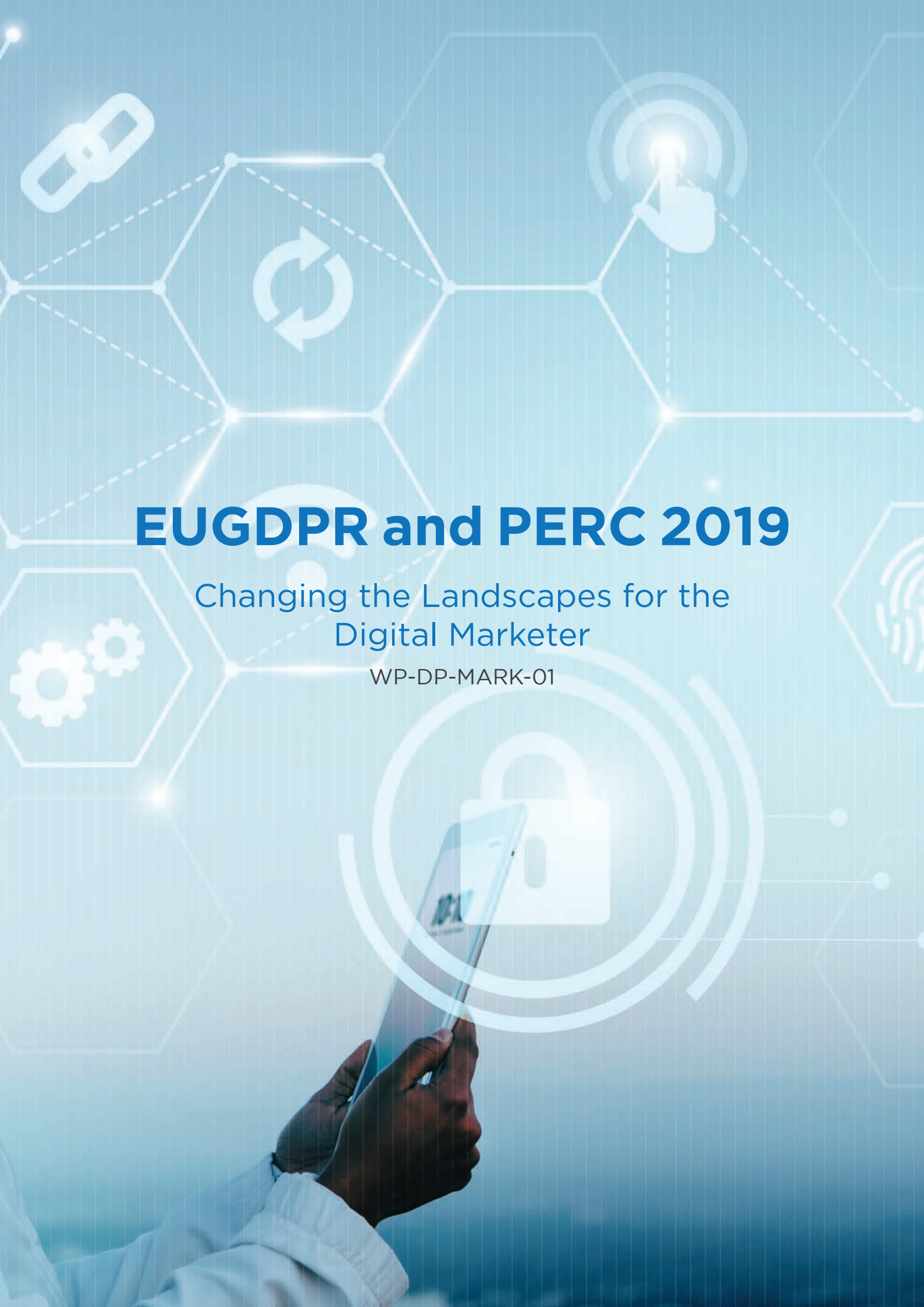
EUGDPR and PERC 2019

Changing the Landscapes for the Digital Marketer

WP-DP-MARK-01



INDEX

INDEX

[1] The Changing Landscape For Digital Marketers

Not a day goes by where there isn't a news headline about brand owners not doing what they should to protect the rights, freedoms and interests of their customers, clients, supporters and employees. And what we're witnessing right now is the impact EUGDPR is having across the globe. Whilst EUGDPR was conceived within the EU, it can be said that many countries around the world have been looking at their own data protection, privacy and security laws specifically following the Facebook/Cambridge Analytica scandal. Such international reviews will cause specific hot topic for marketers working on an international and country specific basis.

Many commentators have described the EUGDPR as the biggest shake up in data protection, privacy and security standards for over two decades. In many respects, the UKGDPR and the DPA18 is an evolution of best practices gained from Europe.

The consequence for marketers is that they must re-boot their thinking by putting the rights, freedoms and interests of their customers and clients at the centre of their thinking. The UKGDPR places a higher global standard on data protection, privacy and security for the digital age. There's now a higher degree of transparency and accountability required by brand owners in respect of the way in which they process personal data and that control over this data must be replaced into the hands of customers and clients. This article will address 6 hot topics around UKGDPR that are causing most interest amongst marketers. The article has also been written with the view of the implementation of the United Kingdom General Data Protection Regulation (UKGDPR) which will come into force on Brexit.

Re-wiring the contractual and legal relationship between the Data Controller and the Data Processor in the Value Chain

In the past, outsourcing could be strategic or tactical, such as IT or payroll processing. However, over time, it's become much more a strategic issue, not simply one based on cost savings.
Under the UKGDPR, the data controller – the client in this relationship that makes decisions as to purposes and means for processing personal data - is responsible for data protection, privacy and security at every point of the value chain[1].

[1] Art. 24, UKGDPR

There are a raft of duties and responsibilities to data subjects whose personal data it processes. This includes, for example, how it will collect personal data, how it will later deal with this personal data across many types of processing and how it provides access to the personal data for data subjects.

Appropriate technical and organisational measures must be in place, including a data protection policy, in order to ensure compliance with the UKGDPR.

And this also means that the data processor contracted to carry this out on behalf of the client must commit to maintaining the highest standards expected and act only in accordance with the written instructions of the data controller[2].

The stakes have been raised by the UKGDPR in that both the data controller and the data processor are jointly and severally liable by law for any personal data breach as a result of their joint activities. It's no longer a matter of contract where liability now falls, as both are held to account.

Pre-UKGDPR

Under an outsourcing contract, the FMCG client contracts with a fulfilment house to process customer personal data from a variety of sources for an international marketing campaign. Any non-performance of the data processor is a contractual matter and not one regulated by law. Responsibility for compliance with data protection rules is a matter for the client.

Post-UKGDPR

The data processor must provide the FMCG client with sufficient guarantees that it will meet the requirements of the UKGDPR and ensure protection of the rights of the data subjects whose data it's processing on behalf of the client.

This outsourcing contract can't be entered into by the client unless there's clear agreement on the following points:

- The data processor will only process and transfer personal data upon expressed written instructions.
- Ensure staff are committed to keeping personal data confidential.
- Ensure appropriate security is in place to protect the personal data.
- Get explicit agreement from the data controller before engaging with another third party (sub-data processor such as cloud service provider).
- Get any agreed third party to comply with the same responsibilities as imposed by the data controller under the UKGDPR.
- Support the FMCG client to achieve compliance with respect to data subject rights.
- Support the FMCG client to achieve compliance with respect to the use and retention of personal data.
- Support the FMCG client in evidencing compliance under the UKGDPR.

[2] Art. 28, UKGDPR

The contract should also provide that the data controller should manage all incidents and report all personal data breaches for their part of the value chain to the DPO and, if required, to the supervisory authority within 72 hours of finding out about them.[3]

The UKGDPR lays down that the data processor has to inform the data controller without 'undue delay'. In simple terms, this means within two hours of any personal data breach[4]. There will be some push back from data processors, who will argue that this is impossible and that they need more time.

[2] Data Protection And Direct Marketing – What's Changed?

It's not an under-statement to say that marketers must re-boot their thinking when it comes to data protection, privacy and direct marketing.

Direct marketing isn't just about products and services. It also covers the promotion of aims, ideals and even political opinions. The application of the UKGDPR and the Privacy and Electronic Communications Regulations (PECR) are more important now given the importance of personal data in making direct marketing work.

What is changing is that direct marketing can trigger data protection and other regulatory issues for those who fail to understand and get to grips with the new digital landscape and the legal framework that regulates this activity. The consequences aren't just eye watering sanctions and fines but go much deeper – and can harm brand and corporate reputation. Training is the front-line defence to protecting business continuity for the brand owner and for marketer's data protection training must be mandatory.

From mass marketing to data minimisation

Data minimisation doesn't just extend to the quantity of personal data being processed at any given moment; it applies to all marketing activities. Be focused.

Mass marketing was based on not having to do your homework – treating a large (if not millions) of customers and prospects in the same way in the hope that their behaviour would lead to the desired outcome – the purchase of a product or service. Culture, language and local market conditions were irrelevant to the advertising or TV commercial. Some TV commercials spoken in one language were often dubbed into another to save time and money in the vain hope that 'mass marketing' would achieve its desired outcome.

Then came the internet and the democratisation of having choice to shop around and compare products and services without getting exhausted in the process. This opened up the opportunities to segment potential customers and clients in a micro-way by understanding their attitudes, values, perceptions, beliefs and behaviours in ways that marketers only a decade previously could only dream of.

Then came the internet and the democratisation of having choice to shop around and compare products and services without getting exhausted in the process. This opened up the opportunities to segment potential customers and clients in a micro-way by understanding their attitudes, values, perceptions, beliefs and behaviours in ways that marketers only a decade previously could only dream of.

[3] Arts.33-34, UKGDPR

[4] This is in accordance with best practice as taught on her UKGDPR Programme, Henley Business School (UK)

But with this more sophisticated profiling came greater risk to the privacy of the individual and, as this Paper discusses, stronger data protection, privacy and security regulations where marketing has to be seen through the lens of 'risk' and marketers are now expected to take a risk-based approach whenever thinking about processing the personal data of a customer or client. Whereas gathering vast amounts of personal data may have appeared attractive – even essential – and where technology companies promised new ways to navigate around vast 'data lakes' the direction of travel is heading in the other way. It's now a requirement that only that amount of personal data required to deliver a product or service should be processed. We've all become minimalists. It's not because personal data is a bad thing – it's because it's a resource that doesn't belong to the marketer. So, we can try to control or process it, but we don't own it. At some point, we have to give it back.

Data minimisation doesn't just extend to the quantity of personal data being processed at any given moment but also the access given to those involved in marketing and processing the personal data of customers, clients and prospects – where access to such personal data must be on a 'need to know' basis in order to do their jobs[5].

[5] This is often referred to as the Principle of Least Privilege (POLP)

Market research and 'sugging'

Brand owners can't dress up direct marketing activities as 'research' – selling under the guise of research (known as 'sugging') if the intention is to try and sell its goods and services or to help the brand owner (or others) to contact people for marketing purposes at a later date.

In accordance with the latest guidance published by the ICO[6], direct marketing rules don't apply if a company or organisation conducts genuine market research where, for example, the purpose is to make decisions for commercial or public policy or contracts with a market research organisation.

However, market research companies will still need to comply with other provisions both in the UKGDPR and DPA18.[7]

The ICO guidance identifies:

"If the call or message includes any promotional material or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. The organisation must say so and comply with the DPA18 and PECR19 direct marketing rules."

Falling foul of this will be a breach of the transparency principle enshrined under the UKGDPR and which permeates the entire Regulation. It could also become a breach of the Telephone Preference Service (TPS) or a breach of PECR, if a text or email has been sent without consent or is instigated by the brand owner for someone else to do so.

List broking

Companies and organisations can use a list-broker service if THEY comply with the UKGDPR, as well as relevant codes of conduct. What that means in practice is that your brand needs to be identified to individuals on the list when they provide consent.

To begin with, there are a large number of sources that can generate leads – phone directories, chambers of commerce directories, previous customers and clients, individuals who've shared an email address, registered on a website, subscribed to offers or news alerts, who've signed up to read a blog, downloaded an App, entered a compensation or prize draw and used a price comparison website to obtain a quote for a product or service.

The guidance from the ICO is that a company or organisation may be able to use these sources provided that they comply with the UKGDPR data protection principles, the DPA18, PECR and of course any Codes of Conduct that would apply within the particular industry or sector.

"It must always act fairly and lawfully," is a mantra often repeated by the ICO on this point.

What this means in practice is also spelt out in Art.14, UKGDPR that deals with the situation where personal data of the customer or prospect is processed, but comes via a third party, such as a list broker, rather than directly from the individual.

---

[6] See https://ico.org.uk/media/for-organizations/documents/1555/direct-marketing-guidance.pdf

[7] This includes processing individually identifiable research data fairly, securely and only for research purposes.

A Data Privacy Notice is required to be given to the individual by the brand owner and this sets out clearly and in easy to understand language the identity and contact details of the data controller, the DPO and also third parties who are recipients or categories of recipients that will receive this personal data. It also covers any international data transfers, what appropriate safeguards are in place if this was to happen to a non-adequate country, as well as list of other rights and freedoms and how to make a complaint.

Where list brokers tend to fall down is that they are harvesting personal data in the first instance and then looking for a customer for this personal data, rather than telling the individual data subject about the identity of this brand owner (customer) at the point of collection of their personal data.

This sounds a bit like 'chicken and egg' but ICO guidance on this point is very clear:

"If you're buying a 'consented' marketing list, the consent request must have identified you specifically. Even precisely defined categories won't be enough to give you valid informed consent under the UKGDPR definition. You must keep records to demonstrate what the individual has consented to, including what they were told and when and how they consented. If you buy personal data from another organisation, you must provide people with your own transparency information detailing anything that they haven't already been told."

This underlines the importance of transparency, accountability and control in the hands of the data subject.

It's clear that responsibility for data protection, privacy and security rests squarely on the shoulders of the brand owner at every point in the value chain. In practical terms, the marketer must do their own due diligence and check that the list broker or other third party has acted in accordance with the higher standards of data protection, privacy and security as demanded under the UKGDPR and has obtained that data lawfully and fairly. And that means individuals have understood that their personal data would be passed on for marketing purposes and that they were given the necessary consent.

And where the direct marketing activity uses texts, emails or automated calls, there's a higher standard that marketers must comply with as they must have very specific consent for this type of direct marketing. Indirect consent (i.e. consent given to a third party like a list broker) isn't going to be sufficient.

The ICO also warn that the 'soft opt-in' exception under PECR doesn't apply for email or text marketing for contacts on bought-in lists. In many ways, there's an 'expectation test' to satisfy – would the person receiving this direct marketing expected to have received it? It's about seeing the world through the eyes and ears of the data subject.

It may be that buying such lists is now 'too hot to handle' and the brand owner may want to invest in building their own B2C direct marketing lists rather than spending resources on third parties to do the job for them.

Interns and students could be trained to harvest this information carefully. The starting point could be to compile lists of customers that have bought goods or services in the past, registered on the brand owner's website or made an enquiry. However, marketers can't assume that individual customers have consented to marketing and so consent will be required. It will be important to record what they were told, and when and how they consented to the use of their personal data.

And of course, brand owners should screen against a TPS list where they're thinking of calling the customer by phone, just in case the customer has joined the TPS list. Calling them regardless would be a breach that would lead to a sanction/fine.

It's also good practice for marketers to hold a suppression list, as this records who doesn't want to be contacted by direct marketing, given that it's an expression of the individual's right to object to the processing of their personal data for that context.

Consent on steroids

The nature of consent has been beefed up and if brand owners want to rely on consent, then be prepared to satisfy the higher bar as a result of the UKGDPR!

Even if able to comply with these higher consent standards, the brand owner must also comply with all seven data protection principles and simply relying on consent of the data subject won't negate this requirement[8]

For example, relying on the consent of a data subject won't legitimise collection of personal data that isn't necessary in relation to a specified purpose of processing. This is fundamentally unfair.

UKGDPR

Art.6, UKGDPR provides six lawful bases for processing personal data, with consent at the top of the list. This isn't some random list of legal bases for processing personal data, although lawyers argue that each ground is equally valid given the circumstances that are the most appropriate for processing personal data.

That said, marketers will be hard pushed to find a ground that so satisfies transparency, accountability and control in the hands of the data subject. Consent in this respect is extremely useful for the brand owner but is by no means the only legal basis. There may be more appropriate grounds, such as legitimate interests, although all of them are challenging to meet in their own ways.

Art.7, UKGDPR provides the conditions for valid consent and in April 2018, Article 29 Data Protection Working Party published its guidance on consent.[9]

Art.4(11), UKGDPR stipulates that consent of the data subject means any:

- freely given
- specific
- informed
- 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 evidential burden isn't on the shoulders of the data subject but the data controller. This is a game changer when there's a complaint made, and the brand owner has to 'prove its innocence' as the presumption will be in favour of the data subject.

[8] See http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[9] Ibid

Consent is central to the rules on direct marketing. Brand owners will generally need an individual's consent before they can send marketing texts, emails or faxes, make calls to a number registered with the TPS, or make any automated marketing calls under PECR.

They will also usually need consent to pass customers details on to another organisation under the first data protection principle under the UKGDPR[10].If a brand owner can't demonstrate they've got valid consent, then continuing to process this personal data will be a breach of data protection laws.

To be valid, consent must be knowingly and freely given, clear and specific. Marketers should keep concise records of what an individual has consented to, and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint. Maintaining accurate and up-to-date records is essential.

'Freely given'

Higher standards means that the data subject must have a genuine choice over whether or not to consent to marketing.

Marketers shouldn't coerce or unduly incentivise people into giving their consent or indeed penalise anyone who refuses to give their consent. It should be as easy to remove consent as it was to give it in the first place. Where consent to marketing is a condition of subscribing to a service, the brand owner will have to demonstrate how this indicates that consent was freely given (it won't be assumed).

In its guidance, the ICO recommends that brand owners don't make consent to marketing a condition of subscribing to a service, unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent can't be sought separately.

It's also relevant to consider whether there's a choice of other services and how fair it is to link consent to marketing with subscribing to the service. It will also be important to assess whether this approach creates an imbalance in the rights and interests between the individual and company or organisation.

'Specific'

In the context of direct marketing, consent must be specific to the type of marketing communication in question (e.g. automated call or text message) and the brand owner sending it.

'Informed'

Data subjects must understand what they're actually consenting to.

Brand owners must make sure they clearly and prominently explain exactly what the person is agreeing to, if this isn't obvious. "Including information in a dense privacy policy or hidden in 'small print' which is hard to find, difficult to understand, or rarely read will not be enough to establish informed consent," says the ICO. This links to the fairness requirements found in the first data protection principle of the UKGDPR.

[10] Under Art.5 (1) (a), UKGDPR personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This is known as the 'lawfulness, fairness and transparency' principle.

'An indication signifying agreement'

Consent must be a positive expression of choice, gone are the days of implied consent. If your boxes are still automatically checked then you WILL fall foul of the UKGDPR.

It doesn't necessarily have to be a proactive declaration of consent – for example, consent might sometimes be given by submitting an online form, if there was a clear and prominent statement that this would be taken as agreement and there was the option to opt out.

But brand owners can't assume consent from a failure to opt out unless this is part of a positive step such as signing up to a service or completing a transaction. For example, they can't assume consent from non-response to an email, as this wouldn't be a positive indication of agreement.

Privacy and Electronic Communications Regulations (PECR)

Marketers must never assume that 'consent is for life', as under the new data protection landscape, consent doesn't last forever!

The notion of consent in PECR and the proposed E-PR remains linked to the notion of consent in the UKGDPR.[11]

However, according to the ICO, the interpretation of consent in a direct marketing context with respect to electronic marketing calls or messages must satisfy an even higher standard and requires the recipient to have previously notified the brand owner that (s)he consents for the time being to such marketing communications being sent by or at the instigation of the brand owner.

"In our view, this means that consent for electronic marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific," says the ICO in its guidance.
In practical terms, this means the customer or client must notify consent to the brand owner by actually sending the direct marketing communication. A company or organisation must therefore be very careful when relying on indirect (third party) consent that was originally given to another company, such as a list broker (see above).

"The person must have intended for their consent to be passed on to the organisation doing the marketing" advises the ICO.

Consent for a one-off message, or consent that's clearly only intended to cover a short period of time or a particular context, won't count as ongoing consent for all future marketing messages. Consent 'for the time being' is given its literal meaning, implying consent lasts as long as circumstances remain the same, and will expire if there's a significant change in those circumstances. In many respects, that's common sense.

[11] Art.4(11) and Art.7, UKGDPR. Besides the amended definition in Art. 4(11), UKGDPR there's details in Art.7, UKGDPR for the conditions for consent and further explanation in Recitals 32, 33, 42, and 43, UKGDPR as to how the data controller must act to comply with the main elements of the consent requirement. Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

An important point for marketers to remember is that the customer or client must specifically consent to the type of communication in question. In other words, the brand owner can't make an automated call to the customer, client or prospect unless that person has consented to receiving automated calls and the brand owner can't send a text unless they've consented to receive marketing texts. Consent to receive marketing phone calls can't be extended to cover texts or emails, and vice versa. Equally, a general statement of consent to receive marketing might be valid for postal marketing but won't cover calls or text marketing messages.

Is implied consent dead?

Marketers can't rely on 'implied consent' as a euphemism for ignoring the need for consent, or assuming the customer or client consents in the absence of any complaint.

The ICO doesn't say it's dead but its guidance tends to indicate that it is.

"Even implied consent must still be freely given, specific and informed, and must still involve a positive action indicating agreement (e.g. clicking on a button or subscribing to a service). The person must have understood that they were consenting, and exactly what they were consenting to, and must have had a genuine choice – if a condition of subscribing to a service is giving consent to marketing, the organisation will have to demonstrate how this indicates that consent was freely given."

On reading this, it sounds very risky to rely on implied consent. The ICO recommends that brand owners don't make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent can't be sought separately. On reflection, the presumption is clear. Marketing isn't necessary.

It's also relevant to consider whether there's a choice of other services and how fair it is to couple consent to marketing with subscribing to the service. It will also be important to assess whether this approach creates an imbalance in the rights and freedoms of the individual versus that of the brand owner.

In some other contexts, the intended use of personal data is so obvious that the act of providing the data in the first place is enough to indicate consent – e.g. providing a postal address when completing an online transaction clearly indicates consent to use that address to deliver the goods. It might be clear that the use of that personal data is a necessary part of a service or activity – e.g. if a website displays a clear banner saying that using the site will result in cookies being set, then clicking through the pages is likely to indicate implied consent to the use of those cookies, as long as sufficient information is made available to fully inform users. However, direct marketing is highly unlikely to form an obvious or integral part of another service or activity in the same way. It will be difficult to show that a customer or client understands they are agreeing to receiving marketing messages unless there is a very clear statement explaining that their action will be taken that way, and a free choice of whether or not to consent.

"It is not enough for implied consent if such a statement is only provided as part of a privacy policy or notice which is hard to find, difficult to understand, lengthy, or rarely read. The customer will be unaware of what they are agreeing to, which means they are not informed and there is no valid consent" advises the ICO.

In practical terms, marketers must ensure that clear and relevant information is readily available to their customers and clients, explaining exactly what they're agreeing to and what choices they have.

In summary, implied consent in the context of direct marketing messages isn't necessarily an easier option for the marketer and is likely to require brand owners to take similar steps for explicit consent.

For example, if explicit consent can be obtained using an opt-in box, implied consent is still likely to require a prominent statement paired with an opt-out box. The ICO therefore recommends that companies and organisations use opt-in boxes in order to obtain explicit consent.

So, perhaps implicit consent has just been read the last rites?

[3] Marketing texts, emails, location data and cookies

Consent is King

Direct marketing covers the promotion of aims and ideals as well as the sale of products and services. This means that the rules will cover not only commercial companies but also not-for-profit organisations (e.g. charities, political parties, etc.).

In many cases, companies and organisations will need consent to send people marketing, or to pass on their personal details. Brand owners will need to be able to demonstrate that consent was knowingly and freely given, clear and specific, and should keep concise records of consent.

Consent is one sixth of the lawful bases for processing personal data, but there are alternatives that can be considered. For example, you may be able to rely on 'legitimate interests' to justify some of your business-to-business direct marketing activities.

However, sometimes companies require consent to comply with the Privacy and Electronic Communications Regulations 19 (PECR). Neither the Data Protection Act 2018 nor PECR ban the use of marketing lists, but brand owners must take steps to ensure a list was compiled fairly and accurately reflects peoples' wishes.

For marketers, a key area of interest concerning UKGDPR relates to the lawful basis for the processing of personal data. UKGDPR outlines six such bases, but in most cases, marketers only need to focus on two: consent and legitimate interests.

Consent represents an important change from PECR. Under UKGDPR, the standard for consent is high. Pre-ticked boxes are no longer legal, as the data subject must be proactive in giving consent, the consent must be unambiguous and freely given, which means it's no longer permissible to make the provision of a service conditional upon a data subject providing consent.

UKGDPR also requires that when data processing occurs using consent as a lawful basis, the personal data must be specific – consent is no longer a catch-all thing. The same principle applies to data privacy notices.

UKGDPR additionally provides regulation in the right to be forgotten[12] and subject access requests.

Legitimate interest relates to the processing of personal data when that processing is necessary for the legitimate interests of the data controller or for society, providing such interests are not overridden by the rights, freedoms or interests of the data subject.

In other words, if it can be shown that the processing of personal data is in the legitimate interests of a brand owner, then the processing of that data may be lawful, but this area is a minefield!

[12] This is referred to as the Right to Erasure,

For one thing, this basis is only lawful if you're processing personal data in ways a data subject would reasonably expect.[13] In addition, such processing must be necessary – if there's another way of achieving similar results this may be a better option![14] In any event, marketers must keep a record of their legitimate interest. There are further considerations too, but these three areas make good starting points for marketers.

Many people ask about UKGDPR, the effect it will have, and the actions needed to take. The following are four of the most commonly asked questions from marketers relating to preparation for the UKGDPR:

Question 1: Do I need to add a double-opt when adding new subscribers?

Answer: The short answer is no. There's no requirement under UKGDPR to have a double opt-in process.

Question 2: Even though not a requirement, is it still a good idea?

Yes. Double opt-in is not a pre requirement of the UKGDPR, although it's recommended as a marketing best practice.[15] It's strongly advisable that a double-opt in process is completed when collecting new data – for example, new subscriptions from a website form. It significantly increases the quality of genuine captured data and it avoids collection of data submitted to forms by online bots or other unscrupulous sources.

Double opt-in is a simple process to implement. The usual process is that on submission of a data collection form an automated email is sent to the submitted email address. The new subscriber data is only confirmed and added to the database on successful receipt and interaction with this email – for example, the clicking of a verification link. This therefore verifies that the email address is both active and actively monitored and that the submitted details are correct.

Many marketers also often include a 'thank you' type of confirmation that the process is now complete. This can also be used to supply additional introductory information or to encourage the new subscribers onwards to the brand website.

---

[13] Often referred to as the 'expectation test'

[14] It's often forgotten but if there's a way of achieving the outcome without processing personal data, then the brand owner needs to have explored this in the first instance.

[15] Source: Direct Marketing Association (DMA). https://dma.org.uk/article/legal-hub-UKGDPR-practitioner-advice-2

New subscribers are generally keen, so it's a good opportunity to advance the relationship. It also serves as a useful positive confirmation to the subscriber that their subscription has indeed been processed.

Marketers may not always want to use the double-opt in. It definitely works for new subscribers. But if marketers are collecting additional personal data from existing subscribers (for example updating preferences or collecting additional profile information such as a birthday or location), they may want to consider turning this option off.

Good as it is, double-opt in does add another step to the process and this potentially introduces an additional point at which interest and opportunity might be lost. However, if in doubt, best to keep it in.

Question 3: Do I need to contact my existing subscribers to re-establish consent?

The short answer is no.

If the conditions of consent were originally gathered in a way which is in alignment with the post-UKGDPR (DPA 18) requirements and that the future intentions for use are also similar, then consent is considered to be continuous.

There's no need to go back and re-establish this just because of UKGDPR.[16]

Question 4: But is it a good idea?

The short answer is – it may be!

It really depends on the circumstances. Consent isn't the only legal basis for processing personal data under UKGDPR, but it's one of the pillars upon which justification is built. From that perspective, it's useful as it's transparent, accountable and evidence of control in the hands of the data subject.

UKGDPR requires that unless there's another justification for processing personal data[17], then data processing can only be done with the consent of the data subject. As well as being a fundamental of permission-based marketing, this isn't dissimilar to current UK legislation and in this respect the principle of consent hasn't radically changed.

However, UKGDPR does extend and clarify the conditions under which consent is given. UKGDPR now requires that consent must be a clear and affirmative opt-in action, freely given with full knowledge of owner and intended purpose of processing. It can't be implied, assumed, bundled or otherwise connected and only applies for a specifically identified purpose.

For brand owners already following a robust permission-based strategy, the new conditions of consent that UKGDPR brings should introduce little in the way of new difficulty.[18]

---

[16] See https://www.guruinabottle.com/enough-already-fed-up-with-UKGDPR-emails-asking-for-your-consent/

[17] Other justifications for processing personal data under the UKGDPR: legal obligation, public interest, vital interest, contractual and legitimate use (Art.6, UKGDPR)

[18] However, a word of caution. So many companies and organisations sent 'zombie emails' to customers and users ahead of 25 May 2018 even when they didn't have to rely on consent. This was seen as 'spam' and didn't lead to consent but rather was ignored. The brand owner can't then try to contact the customer again through other means, given that it deemed consent to be the most appropriate method.

In many respects, UKGDPR is designed to bring everyone closer to the permission ideal, so it's those marketers who are either ignoring or loosely applying the concept of consent who'll need to up their game. In any case, as previously mentioned, consent isn't the only basis for processing personal data.

Legitimate Interest

Legitimate interest is the last opportunity of marketing companies to retain their well-earned marketing lists. This being said, companies and organisations should not have sent mountains of 'reengagement' emails, considered by many as spam. Legitimate interests do away with this.

The UKGDPR also includes a justification under the heading of 'legitimate interest'. This is like the so-called 'soft opt-in' that's commonly used by B2B email marketers under the current data protection laws.[19]

In principle, if a clear, genuine and mutually beneficial relationship is in place, and that the processing is anticipated, appropriate and doesn't otherwise infringe the rights and freedoms of the individual, then personal data processing can still be undertaken without consent. However, the other major change with UKGDPR is that whatever justification we are making for the processing data (consent or otherwise) we need to have assessed the possible impact of this assumption in advance.

The Legitimate Interest Assessment (LIA) is a new feature of the UKGDPR.

Having said all that, many people are taking the opportunity to contact their database to either re-affirm consent, or in the cases where (UKGDPR compliant) consent isn't in place, to establish this.

Some are specifically referencing UKGDPR in this process, but others are simply taking this step as a courtesy – after all, permission is a politeness and re-engaging in this way can be used to show that data protection is an important consideration and serve to strengthen an existing relationship.

There's the danger - in fact a high probability - that some data subjects will also take this opportunity to re-assess their situation and withdraw their consent. So, if marketers take this step, they must be prepared for the loss of such customers and prospects.

On the other hand, re-engaging in this way will have the double benefit of strengthening the bond with loyal subscribers and customers and cleaning out those who are unlikely to engage with the brand owner in the future.

When using opt-in boxes, marketers need to remember that to comply with PECR they should provide opt-in boxes to obtain specific consent for each type of electronic marketing they want to undertake (e.g. texts, emails, etc.)

[19] Privacy and Electronic Communications Regulations (PECR)

Data Protection by Design and By Default

Companies and organisations must now consider privacy by design as a key part of their marketing campaigns, the concept being applied to mass emailing and specific mail shots. Marketers must ensure their program has been designed in line with the requirements of the UKGDPR.

The underlying objective of the principle is to integrate privacy throughout the lifecycle of various technologies and applications that process personal data. At the same time, the practical implementation of data protection by design and by default is tremendously complex because of the uncertainty shielding the meaning of this principle.

In parallel, big data applications, such as predictive analytics in consumer marketing, and more recently, machine learning applications, intensify the interference with the right to the protection of personal data and create the need for 'by design' and 'by default' protection.

Direct Marketing Code (UK)

Within the Data Protection Act 2018, the UK Information Commissioner must prepare a code of practice that contains:

(a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing. References to direct marketing as defined in Section 122 of the Data Protection Act 2018:

Existing customers/clients

One way to ensure explicit consent for existing customers / clients, particularly when processing personal data that's considered highly sensitive, is to employ the use of a double opt-in as discussed earlier.

Double opt-ins essentially involve obtaining consent on two separate occasions as a precautionary measure, a sort of "are you sure you're sure?" that provides a clear paper trail in case of an audit.

Many brand owners have already implemented this mechanism and it's a pretty simple process. Consent is provided by ticking a box and/or filling out a form etc. Then the existing customer / client is sent an email asking them to confirm their interest in receiving further communications from the brand owner. Although not legally required under UKGDPR, using this method is generally seen as best practice particularly when processing sensitive data of the individual in a marketing context.

Profiling customers/clients

Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms.

Under Art.4(4), UKGDPR, profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Profiling in accordance with the UKGDPR comes in three flavours:

General profiling.

In contrast to automated decision-making, profiling is a relatively novel concept in European data protection law. It's now explicitly defined in the UKGDPR (see above).

General profiling refers to the automated processing of data (personal and non-personal) to derive, infer, predict or evaluate information about an individual (or group), in particular to analyse or predict an individuals' identity, their attributes, interests or behaviour.

Through profiling, highly sensitive details can be inferred or predicted from seemingly uninteresting data, leading to detailed and comprehensive profiles that may or may not be accurate or fair.
Increasingly, profiles are being used to make or inform consequential decisions, from credit scoring to hiring, policing and national security.

Ever since the adoption of the EUGDPR in May 2018, debates about profiling have focused on the EUGDPR's potential to limit or offer protection against increasingly sophisticated means of processing data, in particular with regards to profiling and automated decision-making.

While the UKGDPR offers new rights and protection, their scope and limitations are open to debate, partly due to the clumsy syntax of the relevant articles and the lack of authoritative guidance concerning their interpretation.

Decision-making based on profiling.

Profiling and automated decision-making can be useful for individuals and organisations as well as for the economy and society, delivering benefits such as increased efficiencies and resource savings.

They have many commercial applications, for example, they can be used to better segment markets and tailor products and services to more closely align with individual needs.

Medicine, education, healthcare and transportation can also all benefit from these processes.
However, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms that require appropriate safeguards. These processes can be opaque.

Individuals might not know that they are being profiled or understand what's involved, as exemplified by the Facebook and Cambridge Analytica scandal.

Solely automated decision-making, including profiling.

Solely using automated decision-making provides the company or organisation with the ability to make decisions by technological means, without human involvement. Automated decision-making can take place with or without profiling and can be based on any type of data.

The prohibition on fully automated decision-making only applies when the decision based on such technology has a legal effect on, or similarly, significantly affects someone.

If a recommendation about a data subject is produced by an automated process but is reviewed by a human being who takes account of other factors in making the final decision, it's not based solely on automated processing.

However, fabrication of human involvement (e.g. human employees rubber-stamping automatically generated profiles) won't enable a data controller to avoid the general prohibition of automated decision-making, including profiling.

Meaningful oversight must be by someone who has the authority and competence to change the decision.

There are three exceptions to the general prohibition[20]:

- The processing is necessary for the performance of or entering into a contract.
- It is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.
- Is based on the data subject's explicit consent.

It's good practice to provide that information regardless of whether the processing falls within the Art. 22(1), UKGDPR definition of automated decision-making.

Data controllers are instructed to "find simple ways to tell the data subject about the rationale behind, or the criteria relied on, in reaching the decision" by providing information "meaningful to the data subject."

[20] Art.22(2), UKGDPR

The UKGDPR introduces new provisions to address the risks arising from profiling and automated decision making, notably, but not limited to, privacy:

The right to opt-out.

Data controllers must act affirmatively to provide data subjects with access to "at least the right of human intervention", even in cases where one of the Art.22, UKGDPR exceptions applies. Data controllers must provide a "simple way for the data subject to access these rights" that will enable the data subject to express their view and contest a decision.

B2C & B2B texts and emails

There's some confusion as to what the rules are with regards to email marketing and the level of consent brand owners need to email contacts on their database.

One way of cleansing personal data used for marketing purposes is through re-permissions, although consent shouldn't be the default position, as other more appropriate bases for processing personal data may be available.

So, the process of seeking re-permission should still be done with care to avoid becoming a 'zombie marketing email'.

B2C marketing online

B2C direct marketers will need to demonstrate how their company or organisation meets the lawful conditions. Where B2C online marketing is concerned, the new data privacy laws completely change the way we think about handling personal data. If a brand owner can't prove how they've obtained consent from the customer to receive marketing, the likelihood is that they'll be fined if sending this marketing to them.

The key is for B2C direct marketers to comply with all seven data protection principles. The collection of personal data needs to be relevant for the purpose. This means if you have run a campaign or competition you can only use the personal data for that purpose. Creating another purpose to use that information for will need further consent from the data subject.

This is bad news for B2C marketing, as a common practice has been to grow databases using these methods. In terms of marketing databases, these will need to be cleansed and reviewed to ensure an organisation can identify if consent has been granted lawfully and fairly, whether it's being used for explicit and legitimate purposes, what personal data has been collected and the accuracy of that information.

Location data

Location data is referenced with the DPA18 as 'profiling', meaning any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Cookies

A brand owner based in the UK is likely to be subject to the requirements of the UKGDPR even if their website is technically hosted overseas and vice versa.

The Privacy and Electronic Communications Regulations 2019 (PECR) cover the use of cookies and similar technologies for storing and accessing information on a user's equipment such as their computer or mobile. PECR requires that users' or subscribers' consent and there's now a higher standard of consent as a result of the UKGDPR: an unambiguous expression of wishes, freely given, not conditional, as well as some form of affirmative action is required. This may involve clicking an icon, sending an email or subscribing to a service. The crucial consideration is that the individual must fully understand that by the action in question they will be giving consent.

Organisations based outside of Europe with websites designed for the European market, or providing products or services to customers in Europe, should consider that their users in the UK and Europe will clearly expect information and choices about cookies to be provided.

Web Scraping

Web Scraping[21] is a technique employed to extract large amounts of data from websites whereby the personal data is extracted and saved to a local file in the marketers', or to a database in table (spreadsheet), format.

Data displayed by most websites can only be viewed using a web browser. They don't offer the functionality to save a copy of this data for personal use. The only option then is to manually copy and paste the data - a very tedious job that can take many hours or sometimes days to complete. Web Scraping is the technique of automating this process, so that instead of manually copying the data from websites, the Web Scraping software will perform the same task within a fraction of the time.

Screen Scraping

One of the issues the Payment Services Directive 2[22] addresses is Screen Scraping, which is a process of collecting data that appears on the screen from one application to translate it into the display of another.

For example, let's say that a company wants to create a mobile app or a new interface that gives users of the mobile app access to their bank account. They can use screen scraping software that will collect data from the bank's interface, translate it to their own, and then provide a better interface with the same inputs and outputs of data. This sounds sinister and potentially hazardous for the protection of client data in case of malicious use of mobile app technology, however there are a lot of important reasons to use screen scraping, if used with the consent of the end consumer.

Screen scraping can be used by third-party fintech companies and the banks themselves to create interfaces that will provide direct automated access to a user's bank account. As such, with the customer's permission, screen scraping can be used to automate access to their online services through the front door, without creating specific back-door direct access software, something that might be costly and time-consuming.

However, due to the possible issues arising from malevolent use of this technology, in February 2018, the European Banking Authority announced its intention to outlaw this practice in one of their Regulatory Technical Standards that complement the PSD2.

Internal impacts on inter-departmental relationships

The impacts of increased data protection laws are widely felt throughout a company, specifically within the compliance, marketing and sales departments.

It's a tough job for any compliance department to 'bring along' both sales and marketing within one swift action. Ideally both sales and marketing should be approached together although this is not sometimes possible. The key is to identify primary stakeholders within each department, sit them down and discuss the implications of data protection for each of their operations.

e.g. sales/marketing with compliance?

---

[21] This is also known as Web Data Extraction and Web Harvesting

[22] See https://www.ukfinance.org.uk/wp-content/uploads/2018/01/Frequently-Asked-Questions-on-PSD2-and-Open-Banking.pdf

[4] Lead generation for digital marketers

Generating leads

It's important to have your legal team write up an agreement to be signed by each sales lead vendor, providing an assurance they're in compliance with the GDPR before running any EU campaigns.

Marketers should start by identifying all third-party sources using external lead forms. Then, make a simple table containing columns with these headings:

Sources/partners/vendors	In this column, list any source or partner that captures personal data from individuals in the EU, Switzerland and/or the U.K.
Contact information	List the names and email addresses etc. of your contacts at the organisations in this column.
Compliance with GDPR/ PECR	In this column, identify each source as either Y for "currently compliant" or N for "not yet compliant."
Compliance with cross-border data rules	In this column, identify each source as either Y for "currently compliant" or N for "not yet compliant."
Date scheduled for compliance to be fully implemented	For those sources, partners and vendors that you marked with N's for "not yet compliant," find out when they will be ready, write that date in this column and then check back when that date arrives.

GDPR specifies that organisations must maintain clear records to demonstrate consent. One way to do this is to require your third-party sources to show you the landing pages and forms they're using to present your offers and capture prospect data. Again, companies will want to do this before they start generating leads for any EU campaigns.

GDPR clearly is presenting B2B marketers with some major hurdles. However, each of these challenges only serves to make lead generation better and more targeted, as well as making marketers more customer-focused — and that's a good thing.

Selling and buying marketing lists for campaigns

Companies and organisations may be subject to enforcement action if they can't demonstrate appropriate consent, including to the specific marketing activity proposed, which becomes very difficult to prove when using third party personal data lists.

The Information Commissioner's Office (ICO) in the UK makes it very clear that marketers can't just rely on an assurance – contractual or otherwise – from their list broker that the individual's consent is valid.
Under GDPR, it's the data buyer's responsibility to carry out due diligence on the broker to make sure:

- The personal data is current
- The data broker has permission from the individual to pass their personal data on to you
- The individual's consent for your type of planned marketing is valid
- The consent is recent enough to still be valid

Both the GDPR and the Data Protection Act 2018 create an onus on brand owners to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as tick box exercise and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation.

Creating your own marketing lists

Marketers may want to compile their own in-house marketing list using details of people who have bought goods or services in the past, or who have registered on their website or made an enquiry.

Marketers shouldn't assume that everyone is happy to receive marketing just because they have provided their contact details in the past. Companies and organisations should make it clear upfront that they intend to use data subjects' details for marketing purposes. The best way to get clear consent for marketing is to provide opt-in boxes that specify the type of messages they plan to send (e.g. by email, text, phone, fax or recorded call).

Companies should record when and how they obtained consent and what type of messages it covers. If possible, companies should also record whether the customer is an individual or a company, as different rules apply[23] to both. If this isn't clear, assume they are an individual.

Suppression lists

Marketers must maintain a suppression list of people who have opted out or otherwise told the brand owner directly that they don't want to receive marketing material, similar to Canspam.

Individuals may ask a company or organisation to remove or delete their details from a database or marketing list. However, in most cases the company or organisation should instead follow the marketing industry practice for supressing the individual's personal data. Rather than deleting an individual's details entirely, suppression involves retaining just enough information to ensure that their preferences are respected in the future.

[5] New e-Privacy Regulation (expected Autumn 2020)

What's different?

It's clear that the issue of access to online content being conditional on the user's consent to cookies, and who's responsible for obtaining such consent, are key issues discussed by Member States and ones that European Commission has pushed

The latest version of the e-Privacy Regulation[24] (dated 28/8/18) includes various small changes throughout, especially on the Recitals.

Notable exceptions are the Arts.6, 8 and 10, E-PR that the Bulgarian Presidency of the European Commission has decided to ask for more guidance and asked Member States to choose among several options. There haven't been any changes in the wording of Art.8 and 10, E-PR since they are the subjects of proposed options.

Recital 20, E-PR is important to marketeers, as it explains that the responsibility to obtain consent lies on the entity that makes use of processing and storage capabilities of the device or collects the information. However, the entity can request another party to collect consent on their behalf (i.e. a publisher).

[23] There is still a distinction between B2B and B2C under PECR

[24] E-PR

Direct marketing (Art.16, E-PR)

There's some tidying-up of this Article in its drafting, confirming that Member States understood that advertising presented to an individual, such as display advertising, shouldn't be considered as direct marketing. This is further clarified by Recital 32, E-PR that says that displaying advertising to the general public shouldn't be considered as direct marketing.

However, the Recital still makes the distinction between display ad to the general public and display ad that's directed to any specific identified or identifiable end user.

An identified or identifiable end user is the user that has logged in with a private account or personal log-in. Thus, any targeted ad presented in a log-in environment would be considered as direct marketing and the provisions of Art. 16, E-PR would apply.

Art.16 (2), E-PR, for the soft opt-in, the text now allows the use of electronic contact details obtained in the context of a purchase (as opposed to in the context of a sale).

On the time limit for the use of the soft opt-in exemption, the new wording reads:

"Member States may provide by law a set period, after the sale of the product."

This doesn't change anything significantly and it will again create a patchwork around Europe that the publisher would have to comply/respect different time limits across the EU. There are no proposed changes to the language regarding the common prefix to telemarketing. Similarly, the definition of both direct marketing communication and automated calling and communication systems hasn't changed, maybe because there were no further discussions on the issue.

Relationship with the GDPR?

It's important that brand owners understand the different ways in which the GDPR and E-PR will affect their business.

The current PECR provides a specific set of privacy rules to regulate the processing of personal data by the telecoms sector. Until this is amended, PECR will co-exist with the GDPR (which applies to all sectors including the telecoms sector). There remains some uncertainty in the relationship between the E-PR and the GDPR, which will require clarification.

The E-PR is a proposal for a Regulation on Privacy and Electronic Communications that repeals PECR. It's designed to complement the GDPR with regards to electronic communications data, that qualify as personal data, and will significantly strengthen the online and direct marketing legal landscape.

Initially, the aim was to replace the PECR so that the E-PR would come into force on the same day as the GDPR. However, due to ongoing discussions and various legislative hurdles still to cross, E-PR is more likely to come into force in Autumn next year.

While the GDPR regulates the processing and sharing of personal information, the E-PR addresses the rules companies and organisations must follow when sending electronic direct marketing and using track technologies such as cookies. If adopted, it's proposed that it will be lex specialis to the GDPR, meaning that its terms can override those of the GDPR in case of a conflict.

Summary of main changes:

- It extends the scope of PECR to cover telecoms providers, text and email providers and 'over the to providers (Apps)
- It applies rules to new tracking and e-marketing technologies
- It aligns privacy concepts with the GDPR (consent, data breaches, territorial scope, fines)

The E-PR aims to modernise the law, meaning that not only will traditional telecoms providers be caught, but also text and email providers, internet-based voice and internet-messaging services - "over-the-top" content providers such as Skype, WhatsApp, Facebook Messenger and iMessage.

E-PR will apply to any brand owner that provides any form of online communications service that utilises online tracking technologies or that engages in electronic direct marketing, including non-EU providers, that provide electronic services (free and/or paid) to EU nationals.

It also changes the way electronic communications data is currently regulated by creating separate rules for the use of content and metadata, namely how each is used when consent is required. The proposal also includes new rules for the storage and erasure of electronic communications content.

Consent and E-PR

E-PR will be in alignment with the GDPR's approach to valid consent. This means that for consent to be valid it must be freely given, specific, informed and unambiguous. As with the GDPR, this means that, if relying on consent, anything other than clear opt-in consent to electronic direct marketing won't be valid consent.

Direct marketing and E-PR

The definitions of direct marketing and electronic communications are broader than those in PECR. The proposal distinguishes between B2C and B2B communications. For B2C communications, the proposal requires the sender of the communication to obtain the consent of individuals for direct e-marketing purposes.

In contrast, for B2B communications, the proposal leaves it to the Member States to ensure that the legitimate interest of corporate end users is sufficiently protected from unsolicited communications.

Cookies and E-PR

The new regulation will change the rules surrounding use of cookies, including marketing cookies, with privacy rights being prioritised.

Cookies and tracking for online advertisement will remain lawful but will be governed by clearer rules, giving choices to users from the outset when initially choosing their settings. This will be mean a significant change for internet browser providers like Microsoft and Google. They will require a clear, affirmative action from the end user of terminal equipment to signify his or her freely given, specific, informed and unambiguous agreement to the storage and access of third-party tracking cookies in and from the terminal equipment.

Telephone marketing calls and E-PR

Companies and organisations making direct marketing telephone calls would be required to display calling line identification or present a specific code/prefix indicating that the call is a marketing call.

Relationship between UKGDPR and E-PR

As previously discussed, if the E-PR is adopted as it stands, it will be lex specialis to the GDPR, meaning that its terms can override those of the UKGDPR in case of a conflict.

Many aspects have been drafted in line with the UKGDPR so as to avoid such conflict: the penalties for non-compliance will reflect those in the UKGDPR. End users are granted many of the same remedies as provided by the UKGDPR – the right to lodge a complaint with the ICO, the right to an effective judicial remedy against the ICO, and the right to an effective judicial remedy against a data controller or data processor. A right to compensation and damage is also envisaged and, individuals will also have the right to sue for compensation for 'material or non-material damage' caused by an infringement of the E-PR.

Soft opt-in under E-PR

The current draft of the E-PR retains the soft opt-in exemption but limits it to commercial marketing about the sale of goods or services where the brand owner has obtained the individual's personal details in the course of such a sale.

However, the reference to negotiations has been removed, so this is more restrictive in its scope than its predecessor.

Any electronic direct marketing under the soft opt-in must be limited to marketing similar products or services of the specific entity using the soft opt-in (i.e. not another group company).

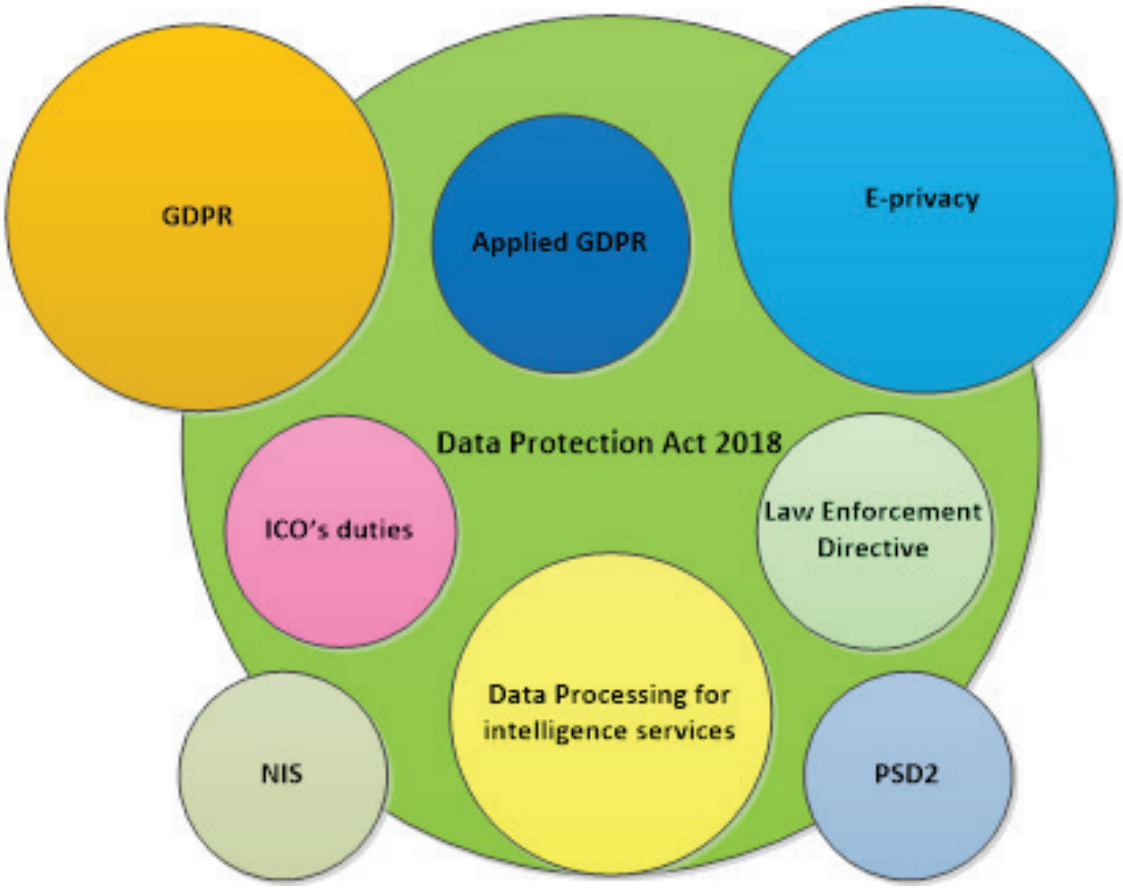
Like the PECR, the marketing materials must be closely related to the products/services originally purchased, and the requirement of providing an individual with a simple and clear option to opt-out in every correspondence from receiving such B2B marketing also remains.

E-PR is one element of the legal data protection eco-system

As you can see from this diagram, E-PR (e-Privacy) is one element of the legal data protection eco-system within EU Member States as well as the UK on exiting the EU in March 2020.

In the UK, the legal eco-system includes new powers of the ICO under the Data Protection Act 2018, Applied GDPR, PECR (e-Privacy), Law Enforcement Directive (LED), the Directive on Security of Networks and Information Systems (NIS), PSD2 and regulations for data processing for the Intelligence Services.

Diagram 1: Data protection eco-system in the UK



Confidentiality of electronic communications

Art. 5, E-PR specifically identifies that electronic communications data shall be confidential. Any interference with electronic communications data, including listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by anyone other than the end users concerned, will be under the latest revision prohibited, except when permitted by the proposed revision.

Consent is now required to process communications content and metadata

The application of the risk-based approach in relation to the processing of personal data under the GDPR to metadata appears to be an effective safeguard against privacy challenges.

The processing of any metadata – irrespective of its source technology or whether it originates from an electronic communications service – can create privacy challenges and therefore may require a data protection impact assessment (DPIA) in line with the GDPR's risk-based approach and accountability principle.[25]

This ensures the nature, scope, context and purposes of the processing of the metadata are taken into consideration. Risks and impacts are identified and safeguards and mechanisms for mitigating that risk are implemented, including a justification for which the data controller can be held accountable.

M2M

E-PR also refers to mobile to mobile (M2M) communication in the context of underlying conveyance.

The proposed definition of an electronic communications service explicitly refers to M2M communication, when dealing with the (technical) transmission service.

Services offering the (technical) transmission of M2M communication should adhere to the confidentiality of communications, even though the message carried may have been composed without direct human intervention.

New business opportunities

The processing of electronic communications data can be useful for businesses, consumers and society.
E-PR broadens the possibilities for providers of electronic communications services to process electronic communications metadata based on end users' consent. This is an opportunity for brand owners as GDPR and E-PR both require brand owners to review what personal data they hold and what personal data they don't require to hold, thus enabling a 'data cleanse' of their data systems.

One of the key principles of both the GDPR and E-PR is that the company or organisation should implement an opt-in policy and have a data subject's consent to process their personal data.

Combined with purging redundant, obsolete or trivial personal data that hinders rather than helps brand owners, marketers will be left with a fine-tuned database of highly relevant leads and customers that genuinely want to hear from them.

[25] The accountability principle is the seventh data protection principle (Art.5, GDPR) and one of the most important sentences in the GDPR

Revised rules on cookies

The responsibility for obtaining consent for the storage of a cookie or similar identifier within the new E-PR lies on the entity that makes use of processing and storage capabilities of terminal equipment or collection of information from end users' terminal equipment, such as an information society service provider or ad network provider.

Companies and organisations may request another party to obtain consent on their behalf. The end user's consent to storage of a cookie or similar identifier may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end user.
Not all cookies are needed in relation to the purpose of the provision of the website service. For example, some are used to provide for additional benefits for the website operator.

Making access to the website content provided, without direct monetary payment, conditional to the consent of the end user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate, in particular, if the end user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other.
Such a trade-off, provided that it complies with the higher standards of data protection, privacy and security, is acceptable.

Conversely, in some cases, making access to website content conditional to consent to the use of such cookies may be considered to be disproportionate and not in accordance with the higher standards of data protection, privacy and security expected by the user.

Consent shouldn't be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, provided that such updates don't in any way change the functionality of the hardware or software or the privacy settings chosen by the end user and the end user has the possibility to postpone or turn off the automatic installation of such updates.

Protection against spam

Spam emails may affect the availability of bona fide email services and could potentially impact the performance of networks and e-mail services, which justifies the processing of electronic communications data to mitigate this risk.

Providers of electronic communications services are encouraged to offer end users the possibility to check emails deemed as spam to ascertain whether they were indeed spam while simultaneously ensuring this does not prohibit the processing of metadata to quantify a level of quality of service requirements.

[6] What's in store for global marketers over the next 24 months?

Growing importance of data ethics in global digital marketing

The storm clouds gathering over many social media sites and app developers worldwide, as well as brand owners that traditionally followed a strategy of 'big data', is now a matter of concern.

Simple, adapt to survive, there's no doubt that GDPR is going to shake up the digital marketing landscape. It is therefore important for businesses to ensure they have implemented the changes necessary to comply. With the possibility of a slow-down in progression, marketeers must ensure their business is ready to adapt and shift in order to tackle this. Don't just accept it, do what you can in order to drive business development and sales. Plan ahead. The troubles facing Facebook and Google [26] post-GDPR are just the tip of the iceberg when it comes to worldwide privacy under threat.

It's now time to re-boot marketing thinking in light of the legal challenge against 'surveillance capitalism' as well as the higher standards now expected from brand owners, post-GDPR.

And what's more, marketeers have known this was coming and would be affecting them in due course.

The lack of awareness regarding peer-dependent privacy is one way that London-based Cambridge Analytica Ltd. was able to collect the personal information of more than 71 million Facebook users, even though only 270,000 of them agreed to take the now-bankrupt company's app-based personality quiz.

"Cambridge Analytica reportedly knew what it was doing [27] but any company that accesses customer data, such as contacts, call logs, and files, can unknowingly breach peer privacy. Blame apps. Virtually all large companies offer apps to their customers, and most of those apps access and collect customer data [28] Often, that includes peer data, which also is collected even though the app's owner may have no direct relationship with the user's peers," say the authors of this article that recently appeared in MIT Sloan Management Review.[29]

Regulator enforcement actions over the next 12 months

The drive for enforcement of data privacy principles must be a key factor for governments and supervisory authorities. The UK's ICO is making it clear to businesses that it will not tolerate non-compliance and marketing is a prime target. As part of their investigations to political manipulation through 'marketing', the ICO served its first enforcement notice since the GDPR came into force on 25 May 2018. The notice was served on AggregateIQ Services Ltd, an online behavioural advertising service provider, which is based outside the EU in Canada. The notice is in connection with online political messages sent to UK citizens during the Brexit campaigns by Aggregate IQ.

---

26 Google hit with €4.3bn Android fine from EU https://www.bbc.co.uk/news/technology-44858238

27 https://www.wired.com/story/whistleblowers-on-cambridge-analytica-and-the-question-of-big-data/

28 https://www.nytimes.com/2017/05/03/technology/personaltech/how-to-protect-your-privacy-as-more-apps-harvest-your-data.html

29 Your Customers May Be The Weakest Link In Your Privacy Defenses by Kolah, A; Kamleitner, B; Mitchell, V and Stephen, A (2018), MIT Sloan Management Review https://sloanreview.mit.edu/article/your-customers-may-be-the-weakest-link-in-your-data-privacy-defenses/

The enforcement notice requires Aggregate IQ to *"cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise, for the purposes of data analytics, political campaigning or any other advertising purposes"*.

New rules on claims management cold calls

New rules entered into force from 8 September 2018, by way of amendments to PECR under Section 35 of the Financial Guidance and Claims Act. These rules require that marketing calls by claims management services can now only be made with the prior opt-in consent of the recipient. These rules also apply where the calls made relate to advice, financial services, representation of people or making introductions or inquiries.

Holding individual directors to account

Regulations amended PECR and give the ICO increased powers to impose direct fines of up to £500,000 on rogue individual directors. Directors will be personally liable for PECR breaches relating to the use of automated calling systems and unsolicited direct marketing where they have consented to or connived in the breach, or the breach is attributable to their neglect. The Regulations came into force on 17 December 2018.

The ICO will monitor the number of complaints it receives about marketing by a particular organisation, to gauge the level of action. A single badly managed campaign resulting, for example, in a number of complaints from recipients, could be enough to trigger investigation by the ICO. Another factor likely to lead to ICO action is an organisation's failure to take appropriate remedial steps as directed by the ICO.

Investigations will be thorough and penetrating

There will be no getting away with anything. Marketers can expect to be asked to answer detailed questions on, and provide evidence for, the source of the marketing data they use, the lawful basis for the marketing e.g. LIA's, the total numbers of different marketing communications sent or made to individuals over the course of the past year, as well as about the number of opt-outs and complaints received and how these where handled. Further questions are likely to focus on the policies, procedures and training within the company.

Leave UK fined £135,000 in Feb 2019

More than 1 million emails were sent to Leave.eu subscribers, containing marketing material which raised concerns with the ICO regarding personal sensitive data being gathered for political purposes. The ICO are investigating how personal data was processed as well as staff training. The directors will also be investigated

Use of alternative legislation for custodial sentences

Many marketing companies will be of the opinion that the GDPR, DPA18 and PECR do not have custodial options for the courts to pursue. This assumption should have altered recently following the sentencing of an individual. A motor industry employee has been sentenced to six months in prison in the first prosecution to be brought by the Information Commissioner's Office (ICO) under legislation which carries a potential prison sentence.

Mustafa Kasim, who worked for accident repair firm Nationwide Accident Repair Services (NARS), accessed thousands of customer records containing personal data without permission, using his colleagues' log-in details to access a software system that estimates the cost of vehicle repairs, known as Audatex.

People who think it's worth their while to obtain and disclose personal data without permission should think again.

Impacts of regulatory actions

Originations who face impending investigations or financial penalties from the ICO will find trading in the future difficult, as customers will tend to migrate to competitors, who may have suitable data protection systems or have just not been highlighted yet. Cambridge Analytic (CA) will be remembered in history as the example of when marketing got it wrong. As soon as the ICO published their requests for information, CA's customers began to turn away, contracts were cancelled or terminated mid research. The main data brokers removed their services and the company was left high and dry.

The large press coverage and political involvement also drove clients away and following the removal of all company assets by the ICO, the company had no way of contacting anyone – basically a dead company. What this demonstrates is that when the ICO investigates a company, the damage is enormous. But ask yourself, has CA been fined for a breach of data protection? No. The only fines have been for LeaveUK whilst AggregateIQ received a 'stop processing' notice.

Loss of new customers

Marketing companies who have a fine imposed on them will find it very difficult to attract customers as all the company's details will be posted on the ICO's website, which would be the first calling point for any prospective client. This again, was a key factor for Cambridge Analytic whose customers left in droves.

Loss of existing clients

As CA proves, clients will distance themselves as soon as they become aware of any potential regulator involvement. Clients will also ask the company to remove data from servers. Marketing companies must be very careful in completing this request as it would give the ICO additional investigatory requirements e.g. why did you delete the data? Fortunately for CA, they did not allow a potential new client to send data from the US to CA servers, as this data was gained from Facebook and breached Facebooks privacy code.