Marketers' whitepaper

Contents

Follows article 1 and 2

[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 organizations (e.g. charities, political parties, etc.).

In many cases, companies and organizations 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 clear records of consent.

Consent is one six 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 now not 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, then the personal data must be specific – consent is no longer a catch-all thing. The same principle applies to data privacy notices.

UKGDPR also provides regulation in the right to be forgotten[1] 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 and 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!

[1] 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.[2] In addition, such processing must be necessary – if there's another way of achieving similar results this may be a better option.[3]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.

There are people asking 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 marketing best practice.[4] 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 –

[2] Often referred to as the 'expectation test'
[3] 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
[4] Source: Direct Marketing Association (DMA). https://dma.org.uk/article/legal-hub-UKGDPR-practitioner-advice-2

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 include often 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.

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) then they might want to consider turning this off this option.

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.[5]

Question 4: But is it a good idea?

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

The short answer is – it maybe!

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[6], 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. [7]

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.

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

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

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.[8]

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.)

[8] 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 would be 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, 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 data) to derive, infer, predict or evaluate information about an individual (or group), in particular to analyse or predict an individual's 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 focussed on the EUGDPR's potential to limit or offer protection against increasingly sophisticated means of processing data, in particular with regard to profiling and automated decision-making.

While the UKGDPR offers new rights and protection, their scope and limits 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 organizations 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 organization 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[9]:

- the processing is necessary for the performance of or entering into a contract.
- it is authorized 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 and 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."

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

[9] Art.22(2), UKGDPR

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 and avoid becoming a ‘zombie marketing email’.

B2C marketing online

B2C direct marketers will need to demonstrate how their company or organization 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 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 organization 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 information, and accessing information stored, 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, where it must be unambiguous expression of wishes, freely given, not conditional and 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.

Organizations 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[10] 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 marketer's 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

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

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 that the Payment Services Directive 2[11] addresses is Screen Scraping, which is a process of collecting data that appear on the screen from one application to translate it into the display of another application.

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

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

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?