GDPR

A review of compliance through your HubSpot portal

Equinet
THE INBOUND AGENCY

GDPR – A REVIEW OF COMPLIANCE THROUGH YOUR HUBSPOT PORTAL

As a marketing professional and Hubspot user, there are many factors to consider during your journey to GDPR compliance. This guide is intended to equip you with the relevant information needed to ensure all your inbound data processing and handling is GDPR compliant before May 2018.

IN CASE YOU DIDN'T KNOW...

The General Data Protection Regulation (GDPR) is a new set of rules that will replace the Data Protection Act 1998 from 25 May 2018.

The primary objective of the GDPR is to give control back to the subject as to how their personal data is obtained, handled, processed and stored. It applies to both controllers and processors of personal data belonging to EU citizens, regardless of your location.

Infringements of the GDPR could result in fines of up to 4% of annual global turnover or £17m, whichever is larger.

WHAT ABOUT BREXIT?

The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

For non-European businesses, GDPR applies to all data processing of subjects within the EU. In this case, it is better to be safe than sorry and our advice would be, if in doubt, assume GDPR does apply.

WHAT FIRST STEPS SHOULD YOU BE TAKING?

You may already have started on your way to GDPR compliance, but certainly one of your first steps should be to have a clear overview of what data you hold, where it is, and how you obtained it. This can be achieved through an **information audit**. The ICO recommends that you run a full data assessment whereby a member (or members) of the team, document all personal data held on your systems, drives, printed or online, before you begin the 'cleaning' process.

Your contact data is likely to fall into one of the three categories, certainly in a marketing arena:

1. People who have already given clear, affirmative consent
2. People who have previously given some sort of consent, but perhaps not obviously affirmative
3. People for whom you are not aware whether they have given consent or not

CHOOSING A LAWFUL BASIS FOR DATA PROCESSING

From there, you should consider on what lawful basis under GDPR you might continue holding and processing this data, or not as the case may be.

Under GDPR, there are six lawful bases for any business to process personal data - let's look at the most pertinent to you as an inbound marketer here.

Firstly, there are two lawful bases for data collection and processing that are common to all businesses, namely "legal obligation" (for example, processing salary data for your staff) or "contract" (for instance, where you've been asked to send a quote to someone). It's clear which of your contacts you would be handling internally under these provisions.

Consent

Secondly, there is the basis of "consent": an oft-highlighted emphasis of GDPR. There is a higher standard of consent under the new legislation - the understanding that a person will need to be able to freely, unambiguously and affirmatively consent to a business processing their data in a particular way. The benefits to the individual are that they have real choice and control over how their data is used; and for the business getting consent right reflects the importance you place on providing a **great customer experience, built on confidence and trust**.

Yet, with consent having to be fully informed, there is potentially a burden on your business to provide clear and exact detail to individuals as to what that consent means, how data will be processed, stored and used by you (via your privacy information) and how you will inform them if/when this might need to be revised for new activities. You will also have to evidence how and when you acquired consent, how you will update that consent where needed and make it easy for someone to withdraw their consent at any time. (We consider consent, as perhaps the most obvious choice for inbound marketers, in more detail below.)

Example – Networking:

One of the most frequently asked questions surrounding consent concerns receiving business cards at trade shows and events. Does someone freely handing over their information to you in a non-digital format qualify as consent? Perhaps. But unless you've managed to obtain some form of documented, affirmative consent, this is not compliant.

Arguably, one would need to perform a balancing test between legitimate interest and privacy invasion. It is reasonable to expect a 'Nice to meet you' email following the encounter, but to add them straight to your database and subsequently send them your weekly newsletter is far from compliant. A better strategy would be to direct the subject to your website where they can view your privacy policy and find a positive opt-in where they can freely give their consent to your communications.

Legitimate Interest

Lastly, there is the lawful basis of "legitimate interest"; that is to say, the interest or **the stake that the company processing the personal data may have in that processing**. As long as that data is used in a way that people might "reasonably expect" with minimal impact on individual privacy, "legitimate interest" incorporates commercial benefit as a justification for this type of processing. For instance, Recital 47 of GDPR states: "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". (Note: any direct marketing that you undertake must also comply with e-Privacy law - currently the Privacy and Electronic Communications Regulations (PECR) - which requires certain levels of consent with regard to your recipients.)

Happily, just prior to publishing this guide, the ICO finally produced some more specific guidance on how businesses can demonstrate compliance when utilising "legitimate interest". The guidance gives some comfort to those of us in the B2B realm in that it suggests "business contacts are more likely to reasonably expect the processing of their personal data in a business context, and the processing is less likely to have a significant impact on them personally."

Just as for "consent", if you choose this lawful basis, there is a burden of proof on any company opting for this route of compliance, via a **legitimate interest assessment (LIA)**. This LIA is essentially a risk assessment document which records your business necessity in using an individual's data balanced against the impact on that individual of you using their details to forward your "legitimate interests". In addition, again as for consent, you will need to include details in your privacy statements as to how you will be processing personal information and a justification of your business purposes for doing so.

There is a simple template LIA which the ICO has produced which gives you a way to evidence the balance between your commercial interest in processing the data and the individual's rights in terms of data privacy. In addition, he guide produced by Communicator Corp as well as that created by the **DPN** are highly recommended here, both offering sound judgement and direction to business on how you might implement.

Example – Personalisation:

A company relies on consent for its marketing communications, but may rely on legitimate interests to justify analytics to inform its marketing strategy and to enable it to enhance and personalise the "consumer experience" it offers its customers.

DPN LEGITIMATE INTERESTS GUIDANCE – GDPR (Page 11)

HOW CAN HUBSPOT HELP YOU RESOLVE KEY COMPLIANCE ISSUES?

When we consider the principle areas of inbound marketing, there are four key areas for renewed consideration for GDPR compliance. The following is a summary of what new obligations we need to be cognisant of and how we can use both HubSpot functionality and more robust processes to respond to them.

1. DATA CLEAN-UP

We looked briefly above at the information audit, which is a useful first step in terms of GDPR preparation. Thinking about the data in your portal, you will probably have some contacts, who've been with you since you began your inbound journey and who will have clearly consented to receiving your content offers, blogs and newsletters. And there may well be some who are in your databases (other marketing platforms you use) for whom your record of provenance/consent may be less evident.

It's worth noting that, in light of GDPR, HubSpot is introducing a new data field that allows you to allocate a lawful basis to a particular contact, e.g. the lawful basis field for contact A can be marked as "contract", for contact B "consent", for contact C "legitimate interest" etc.

Questions for your consideration:

A Do you or your data processor need to run a re-engagement campaign with all your existing but inactive contacts to ensure continued consent prior to May GDPR deadline? The HubSpot list functionality allows you to select clients with "low engagement" (i.e. have not opened a defined number of emails from you); you may wish to consider mailing them to ask if they would still like to receive your content in future or would they prefer to be removed from your database. It's worth bearing in mind also that HubSpot will remove email hard bounces after a set amount of "bounced" emails, again removing defunct addresses from your campaigns.

B Where there are contacts whom you may acquire via outreach campaigns, networking or trade/industry events going forward, you should consider how "legitimate interest" might be a more appropriate lawful basis via which to engage with them until such time that consent is in place (or they withdraw their consent). To this end, you'll need to consider running a legitimate interest assessment for these contacts, and draw on evidence such as your buyer personas and marketing strategy work as a justification of your interest in using their data (in a reasonable way).

2: CONSENT: OPT-INS, COOKIE POLICY AND PRIVACY POLICY

Under GDPR, the emphasis across the board is on the Data Controller (essentially the one holding the personal data of a "data subject") gaining consent to be able to store, transfer, process and use contact for a named and defined purpose (e.g. for information, for research, for marketing etc). Privacy and cookie policies will need to be clear on these lawful bases for holding and processing personal data, how your data retention periods and that individuals have a right to complain to the ICO (Information Commissioner's Office) if they think there is a problem with the way you are handling their data.

To reiterate, consent needs to be given by data subjects affirmatively, freely and unambiguously. HubSpot provides the tools for us to do this via forms, and - also in the light of GDPR - it has developed new mechanisms for double opt-ins, and settings for those opting out of cookies etc.

In addition, Hubspot enables users to demonstrate records of what consent was given and when, and enables the data subject to withdraw consent at any time, e.g. subscription preferences and unsubscribe functionality included at the foot of all mailings sent.

Questions for your consideration:

A You'll need to evaluate the language used on the consensual tick boxes used on forms to ensure that it is broadened to meet GDPR transparency requirements. Affirmative and unambiguous language should be used giving the user two options. For example, a prospect downloading a gated ebook could be given one option for the download of the eBook and no further communications, and another option for the download of the eBook and further relevant content offers and information in the future. Alternatively, if you are using „legitimate interest" as your basis for processing data, you might wish to include some explanatory text on your form to highlight that this is the case.

B You or your agency may already use consent mechanisms when engaging with your new subscribers and leads in HubSpot. However you may wish to go further to validate consent. Do you want to use double opt-ins for your contacts going forward? In other words, do you want to send a follow-up email to any contact that has signed up or opted-in to receive your content asking them to validate that it was indeed them that asked to received your offers? (Note: GDPR does not legally require you to use double opt-in.

C Do you need to update your Cookies Policy and Privacy Policy? Privacy Policies used to be written more for the benefit of the business they belonged to and have often been relatively opaque in terms of the language used for the data subject. In the light of GDPR, best practice suggests that they should be written for "your mum" so that the data subject is clear on what data is collected by you, how it is used, how it is stored etc. In addition, as mentioned above, you should ensure that you are explicitly covering the lawful basis (or bases) under which you are processing data and what that entails.

3. DATA STORAGE AND PROCESSING

Regulation outlined under GDPR requires you to be clear about what information you hold, how it is processed and to ensure that what you do hold is done securely. In regard to the information that is held in HubSpot you should be aware of its security and resilience processes:

Data Security

HubSpot is rigorous about protecting the data of its customers, hosting its own website on the exact same platform as its users. In addition, it partners with industry-recognised hosting and security service providers to keep the platform safe for customers' content. Full details on the HubSpot security program can be found at **https://www.hubspot.com/security**

This page details: the levels of in-transit encryption used so that customer portal sessions are always protected; HubSpot's use of "enterprise-grade firewalling, routing, intrusion prevention, and behavior analytics capabilities" to protect its infrastructure and its customer sites from attack; and its testing and auditing programme to continually monitor vulnerability to security bugs and respond quickly to flaws.

HubSpot has **recently announced that it is now to house all data for customers-based in the European Economic Area in a Google Cloud data-centre in Frankfurt**, thereby ensuring that data is stored, processed and handled within Europe.

"HubSpot will be leveraging the Google Cloud Platform Frankfurt region to support local customer data, as well as provide outage and data protection as needed. The HubSpot product is made up of over 5,000 microservices, including AI and machine learning infrastructure, behind static front end apps. HubSpot's product team updates these services and apps more than 1,000 times a week on average, constantly improving the performance and customer experience of HubSpot's products. HubSpot's use of Google Cloud Platform in Europe will enable its customers around the globe to benefit from the speed, reliability, and security of Google Cloud."

Data Breach

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. It is worth noting that a company only has to notify the ICO of a breach *"where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage."*

Questions for your consideration:

In addition to your HubSpot portal which holds the majority of your contact data, your data processor may hold other data from previous data transactions. It is recommended that you remove all data that is no longer needed by means of hard-deletion (virtual shredding technique) and that - cognisant of GDPR's "privacy by design obligations", you define a process for future storing and deletion once data has been moved as appropriate.

4. STRENGTHENING OF INDIVIDUAL RIGHTS

Whilst largely still the same as under the Data Protection Directive, the GDPR introduces two new rights for individuals that you'll need to be aware of:

Right to be forgotten (aka right to erasure)

Data subjects can request the deletion of their personal data, where there is "no compelling reason for its continued process" (i.e. this could be where the individual has withdrawn their consent, or their personal data is no longer relevant to what it was originally obtained for).

Right to data portability

Similarly, data subjects will have the right, from May, to demand a copy of their data in a common format (for example, .csv file) so that they might move it to another Data Controller of their choice.

Right to access

Whilst this latter is not a new right, individuals have long had the right to have access to all the data that a body holds on them, the intention under GDPR is to significantly reduce the timescale for processing an access request from the current 40 day period (we're yet to find a precise definition as to what that timescale is reduced to yet!). Again, this information has to be provided to them in an easily accessible format.

Questions for your consideration:

A HubSpot has long had robust facility for data subjects to unsubscribe and opt out from future marketing communications, as well as having a very simple contact deletion procedure. We will need to agree a responsive deletion process; if you are approached as Data Controller with a request for erasure, you should agree with your data processor how you will notify them, what turn-around time is expected to comply, and how you will evidence this.

B Similarly, you'll need to agree a responsive process for those times that you are approached as Data Controller with a request for data portability and/or access to data held. Again, you'll need to agree how you will notify your data processor, what turn-around time is expected, and the format you would like the information to be provided in, for secure transfer.

SUMMARY

The GDPR, in the eyes of many, is a legislative solution that will see an end to unscrupulous and, quite frankly, outdated cold marketing tactics. To that end, it is to be welcomed that all personal data held, going forward, will be of a higher quality and be processed in a way that is conscious of the wishes and requirements of its individual owner.

Whilst compliance might seem onerous, inbound marketers can feel perhaps more confident than many that a permission-based and transparent approach are harmonious with the sentiment of the regulation. By ensuring that you evidence the lawful basis you choose, through legitimate interest assessment, the right language on forms and in your privacy policies, compliance may not be as burdensome as you envisage.