GDPR
(General Data Protection Regulation)

A Brief Guide for Clients

This note is intended to be helpful to Waving Moose clients - generally sole service providers, small businesses, charities and community organisations - in understanding new obligations under the GDPR in relation to the personal data that you hold. Please note that I am neither a lawyer nor a data protection professional and am not responsible for the fulfilment of your legal obligations.

Sam Collins
May 2018

1. INTRODUCTION

What is the GDPR?

The **General Data Protection Regulation** (GDPR) is a new, European-wide law that replaces the Data Protection Act 1998 in the UK, with effect from **25 May 2018**. It places greater obligations on how businesses and organisations - from sole traders to multinationals - handle the personal data of EU Citizens.

The main aim is to give individuals more control and increased personal rights in relation to their data. The general principle is that collected data must be kept to a minimum and its use limited to the purpose for which it has been collected.

Compliance

The GDPR is enforced in the UK by the Information Commissioner's Office (ICO). There will be tougher enforcement action and potentially high fines for breaches. It is recognised that small businesses have fewer resources and pose less of a risk to data protection, so there will likely be more leniency by the ICO in relation to any non-compliance. But you should be aware of your legal obligations and take steps to comply. It will also be helpful to document your 'policy' to demonstrate understanding and willingness to comply.

Guidance

There is a huge amount of information about the provisions of the GDPR on the ICO Website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

This note picks out what I think are the main points for awareness and action by Waving Moose clients, with links to further information throughout.

2. PERSONAL DATA

What is personal data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by it. This would include: name, address, email, phone number, ID numbers, location data or other online identifier (such as IP address).

Do you process (ie collect, hold or use) personal data?

Inevitably yes - in relation to your clients, customers, partners, colleagues, employees etc. GDPR applies to data held electronically or manually.

Further information on definitions : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

3. LAWFUL BASIS

On what basis is it permissible to process personal data?

You must have a valid 'Lawful Basis' in order to process personal data. The GDPR provides six lawful bases:

- **Consent**
  The individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract**
  The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract (eg give a quote).
- **Legal obligation**
  The processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests**
  The processing is necessary to protect someone's life.
- **Public task**
  The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:**
  The processing is necessary for your legitimate interests or the legitimate interests of a third party.

Further information on the lawful bases: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Consent is the aspect of the GDPR that has attracted most attention (see section 4 below). But this can obscure the fact that there are clearly other bases for processing personal data and some, or even all, the data you hold may well fall under one or more of them.

If you are processing personal data for the purposes of legal obligation, contract, vital interests or public task, then the appropriate lawful basis is fairly clear cut. As a small business or sole trader, the most likely of these is **Contract**.

As an example, I hold personal data of my clients for contractual purposes, ie to respond to requests for information, to provide advice and in connection with ongoing work or service for which I am engaged by them to provide. I do not undertake email or other direct marketing. You may be the same, in which case Contract is likely to be your lawful basis.

If you have **staff** or **volunteers**, there are likely to be different lawful bases related to the various ways you use employee data. You need to map the data you hold on your employees to identify what personal data you collect from them, what you process, for what purposes and who has access to it, internally and externally. A good article on this, with some examples, is here: https://www.wirehouse-es.com/2018/02/guide-lawful-basis-processing-employee-personal-data/

If some or all of the personal data you hold does not fall under contract, legal obligation, vital interests or public task, then you are likely to have a choice between using **consent** or **legitimate interests**.

4. CONSENT

If you haven't got one of the other lawful bases, you must obtain **explicit, opt-in consent** from the data subject to process their data and it must be very clear about the **specific purposes** for which you will use it**.**

For example, if you want to use personal data for the purposes of marketing - to existing or prospective customers - you must have obtained their genuine and specific consent for that purpose.

The consent rules are:

- You must **clearly specify** the purposes for which you use a person's details. For example, if someone emails you to ask for information or a quote, you cannot then use their email address to send them marketing material. (Unless you then seek, receive and record their consent to do so).
- You must have their **positive opt-in**, you can no longer use pre-ticked boxes, silence or any other method of default consent.
- You must have a **proven record** that the person has given you permission to use their details to contact them for this specific purpose.
- People must be able to **withdraw consent** as easily as they gave it.

Membership Organisations

If you are a membership organisation then you will be holding the personal data of your members. **You must obtain confirmation from your members that you can use their data.** For new members this should be done when they join. For existing members, you need to seek their explicit consent - strictly speaking now if you haven't done so already, although if this is difficult a pragmatic approach could be to do so at the time of their renewal. You need to ensure procedures are in place for retaining records that evidence this consent. You must tell them what you will be using their data for and give them a clear means of withdrawing their consent.

Charities

The requirements of the GDPR apply across the board in charities, for fundraising, campaigning, marketing, staff, volunteers and recording information about service users – anything that involves processing an individual's personal data. You need to review your processes for getting consent related to all these areas and ensure in all cases that it is explicit, specific and recorded, as above.

Further information on consent : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

5. LEGITIMATE INTEREST

Legitimate interest is the most flexible lawful basis for processing, but it does seem a bit woolly. It effectively allows you to contact people where you or they have a 'legitimate interest'. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification.

So it *may* be possible for you to send direct marketing by post or make calls to numbers not registered with the telephone preference service, provided you can satisfy the legitimate interest condition. Giving people an opportunity to opt out of these will still be acceptable, but that won't mean you have consent – it will rely on legitimate interest and you have to make sure you get this right.

Charities and community organisations may be able to argue this better than commercial interests, but it's a tricky balancing act. Your legitimate interest as a charity in furthering your cause must not override the rights of the individual, so the reasonable expectations of the individual based on their relationship with you must be taken into account. Ultimately, GDPR is very clear that an individual's choice to say "no" is paramount.

You may prefer not to rely on it, for two main reasons:

- The other lawful bases are easier to prove. If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. You would have to be very careful about proving your belief there is 'legitimate interest'.

- There may be a clash with the Privacy and Electronic Communications Regulation (PECR) which is still in force in the UK and which stipulates that you must not send marketing emails or texts to individuals without specific consent.

Further information on legitimate interest : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/

6. HELP IDENTIFYING YOUR LAWFUL BASIS

If you are unsure, the ICO provides an interactive tool to help you decide which lawful basis is the most appropriate for your activities.

https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/

7. DATA MANAGEMENT AND USER ACCESS

One of the other key changes with GDPR is the new emphasis it places on users' right to access their own personal data. In simple terms, this means people can make subject access requests at any time to check the data you hold and what you do with it.

The GDPR also brings in a "right to be forgotten" where people can request the removal of personal data, either if they no longer want you to have it or if it is no longer used for the purpose it was collected. Data has to be kept up to date and accurate so think through how you will make sure you are keeping data for no longer than is necessary.

In practice this is unlikely to be a common occurrence for small enterprises such as yours, but you should at least put a process in place, such as giving people a means to find out what information you hold on them and remove all information about them in your privacy policy.

8. SECURITY

A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures'. You should therefore have in place suitable physical, electronic and managerial procedures to safeguard and secure the information you hold. This includes:

- Securing all new and existing hardware to reduce vulnerabilities and providing only the functionality and services required.
- Having appropriate password security procedures for your hardware and software.
- Having effective anti-malware defences to protect computers from malware infection.
- Routinely backing up electronic information.
- Having boundary firewalls to protect computers from external attack and exploitation and help prevent data breaches.

Further information on security: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

9. ACCOUNTABILITY

Accountability is one of the data protection principles - you are responsible for complying with the GDPR and you must be able to demonstrate your compliance. So you need to put in place appropriate technical and organisational measures to meet the requirements of accountability. For us as sole traders and small organisations, you should at least keep a note on file that states your consideration and response to all this. I have produced one for my own business which I would be happy to share. And you should have a published Privacy Policy on your website and email marketing communications.

Further information on accountability : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

10. YOUR WEBSITE

Here are some specific things you need to consider in relation to your website.

CONTACT FORMS

a) If you HAVE a contact form

If you have any kind of contact form on your website, it must clearly state the purpose for which the data collected is to be used and have a clear and specific positive opt-in to gain consent for that specific purpose.

So, a box needs to be added to seek the explicit consent of the enquirer to collect their data for a specific purpose. For example, if you are just using their data to respond to their query (and, if they then engage you, to provide your services), then you need a tick box (positive opt-in) for that. But if you also want to send them other things, eg marketing emails, then you will also need a separate tick box to get their consent for that.

You must also then have a means for recording that consent in your own systems.

b) If you DON'T HAVE a contact form

People may phone or email you and give their details to enable you to respond to their query, so you must still comply with the GDPR in regards to that. You should include in your Privacy Policy how you deal with that information (see below).

PRIVACY POLICY

a) If you HAVE a Privacy Policy on your website

Your Privacy Policy will need to be updated to reflect the GDPR. You need to consider and specify the Lawful Basis on which you collect and hold personal data. This still applies even if this data is not collected directly on your website via a contact form.

For example, if your Lawful Basis is Contract, your policy should explain that you collect personal data for that purpose (ie to respond to the person's query and, if they then engage you, in the context of the service you then provide). If you also want to use their details for other things, eg marketing emails, you will need to state that you will not do so without their explicit consent (and then - of course - get it and record it). You should say that anyway, regardless of whether you intend to market.

I can make these updates for you, if you confirm to me that this is your Lawful Basis (ie what you use personal data for), or let me know what other Lawful Basis you wish to rely on. (The cost will be charged at time only, unlikely to be more than £20, and would just be added to your annual renewal).

b) If you DON'T HAVE a Privacy Policy on your website

If, for whatever reason, you opted not to have a Privacy Policy when your website was designed, I strongly suggest you have one now. The cost of the additional pages to your website will be no more than £35.

COOKIES

Cookies fall under the framework of GDPR (which now recognises a website visitor's IP address as personal data), but more specifically will be covered by a new ePrivacy Regulation. This was intended to come into force with the GDPR in May 2018, but has not been finalised and not now expected until 2019. We await clarity about cookies therefore until then.

However, it is expected that the ePrivacy Regulation will move away from the existing 'publisher site notice' approach for obtaining consent to one based on the settings of the browser - users will be prompted to choose their privacy settings on their web browser, not on individual websites (ie an end to all those annoying pop-up cookie notices).

GOOGLE ANALYTICS

If you have Google Analytics on your website, Google collects a lot of data from every visit / visitor but it does not store any personally identifiable information. A visitor's IP address is used to determine their physical location but the IP address itself is not data that can be accessed through Google Analytics; all data is aggregated and anonymised. For a standard implementation of Google Analytics therefore - installed with your website design - you do not need to gain specific opt-in consent from users.

If you have separately since added and are using Google's advertising features however, the situation is different and you must comply with Google's new EU User Consent Policy introduced on 18 April 2018 in order to comply with the GDPR.

TESTIMONIALS

If you include Testimonials on your website (or anywhere), you must have (and have a record of) the person's consent for their details to be used for that purpose. If your Testimonials are anonymised and individuals cannot be identified by them, no need to worry.

11. CHECKLIST FOR ACTION

- € I have reviewed the purposes of my data processing activities and selected the most appropriate lawful basis (or bases) for each activity.
- € I have checked that the processing is necessary for the relevant purpose, and am satisfied that there is no other reasonable way to achieve that purpose.
- € I have documented my decision on which lawful basis applies to help me demonstrate compliance.
- € I have included information about both the purposes of the processing and the lawful basis for the processing in my privacy notice.

Consent Checklist

- € I request the explicit consent of every user before any data collection takes place. Requests are in clear, plain, easily understandable language free of legalese. They also stand alone from other matters or requests and are not be buried in other text.
- € I have a clear and accessible privacy policy that informs users how collected data will be stored and used.
- € I have a means for users to request access and view the data I have collected on them.
- € I provide users with a way to withdraw consent and purge personal data collected on them.

12. CONCLUSION

Don't panic, but be prepared! This is all good practice anyway.

Comprehensive information on all the provisions of the GDPR can be found at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/