General Data Protection Regulations (GDPR)

New regulations come in on 25th May 2018.

As a maker whether you operate as a small company or a sole trader and have a mailing list or store the details of past customers and visitors, you should take note there are fines for non-compliance with these new regulations and the use of other people's personal details in a way they didn't consent to. This is applicable to everyone.

You probably don't realise it, but you are a 'data controller' if you (alone or jointly with others) 'process' other people's 'data' whether that's obtaining it, having access to it, using it and even just storing it.

If you have names, addresses, email addresses and/or other information stored, on reference cards or electronically, firstly you should check whether you ought to register with the Information Commissioner's Office (ICO) who keep a public database of 'data controllers' – there's a self-assessment tool on their website you can use to check at https://ico.org.uk/for-organisations/register/self-assessment . Fortunately if you only collect names, addresses and email addresses for your own marketing purposes then you are probably exempt from registering.

You will still, however, need to comply with the GDPR.
You should know and have a written document which lists

- What data is collected? and Why?
- How is it used?
- How and when do/did you tell the people whose data you store what you use it for?
- How do you keep the data accurate?
- Where is it held, for how long and how is it kept secure?
- What do you do if there's a data breach?
- How do you delete it when it is no longer appropriate to keep it?
- If an individual asked to see/delete your record of them or restrict its use, how do you do that?

Notes

1) You are given information for a purpose and that purpose is key. You cannot use the data for another purpose than the one you told the customer you collected it for. Previously you could assume consent or include a small box 'tick here if you don't want to hear from me and my friends'. Now you need to be able to prove active consent.

2) Data 'held' includes information on
spreadsheets/documents saved onto or downloaded on hard drives, laptops, phones, tablets etc
a web site hosted elsewhere (like the Artweeks main database)
old emails mentioning people, their names and phone numbers, e.g.: Outlook; Yahoo etc
Cloud-based data holding and transferring facilities, e.g. Dropbox, GoogleDrive, MailChimp
Cookies on your website

Dropbox/Mailchimp/Google/cloud facilites etc are all data processors as they store data. These are US companies so not subject to GDPR so to use them and comply, you should look for the 'Privacy Shield' that shows they have signed up to EU privacy law. Using Paypal is fine if your site directs a customer into the Paypal site – and you yourself do not provide Paypal with any information.

3) Using data: The principle is when using data is that processing should be lawful, fair, and transparent.
You have to tell people what you are doing or going to do with their data before you do it.
You also need to be clear if you pass information on why you are doing this and that you have consent to do it.

So what should you do?

Collect personal data only for a specific explicit purpose (documented in a privacy policy) with written consent and don't use it for other reasons. Only put people on a mailing list if they ask to be on it. If you have a mailing list, you should check you have a record of consent for each individual or ask each recipient to confirm they agree to you keeping their data for the purpose of sending them information.

Minimise the data held: data should be adequate, relevant and limited to what is necessary to the purpose. Only collect the information that you need and will use.

Have a retention schedule and delete data in a timely way. It is not legal to store data 'forever' or for an unlimited time period 'just in case' however much value you think it could be in the future as it would be for a different purpose.

Keep the data secure. This information is confidential. Only share it with people for whom you have explicit consent to share it with. Don't download information on shared computers, and keep all devices where the information is stored password protected. (Put your external hard-drive in a safe.)

You are required to tell people what information you'll keep and why, how you'll use it, where it's stored, who else has access to it and when you'll delete it – this is your Privacy Policy.

You should have your Privacy Policy on your website separate from any Terms and Conditions and it should include information on cookies .

You are also required legally to be able to show any individual all your records on them in all formats, make a change for them, delete them all or restrict use if asked, within 30 days.

Please note the above has been sent to you by the Guild as guidance only to make you aware of the changes to the GDPR. if you are uncertain about any points mentioned you should seek advice from the ICO website www.ico.org.uk