Well, it's the General Data Protection Regulation which is Europe's new act. It's set to replace the outdated 1998 Data Protection Act.

But what about Brexit? Well, we are leaving but it takes two years. It means that the GDPR will be in place way before we have actually left. The UK released their own data protection bill in 2017 which still implements a lot of the GDPR. The mirroring of the rules means that it's likely to be accepted by the EU. This helps businesses which supply to European clients to transfer data between the two.

Even post-Brexit, if your business, regardless of where it is situated, holds any information from anywhere in the EU then you'll have to follow the GDPR.

What does this mean for the way you handle your customer's data?
This new GDPR impacts you if your business's website has an online shop or collects personal information. You'll be more accountable for your client's personal details, meaning you'll have to have company data protection policies, impact assessments, documents about how you process their information and policies to prevent a security breach.

This means that your clients will have new power to request their information, which you have to comply with within a month:

Privacy rights are changing.
Consumers are now entitled to request a free copy of any data that you have for them. This information should be provided in an electronic format, e.g. .txt file and should also be easily accessible.

Communication is key!
As previously discussed, a big part of the GDPR is communicating with your users about why you're collecting and using their data. Be clear and concise to prevent confusion, and give them a way to request a copy of the data you hold, or to have it deleted if they wish. You will need to update your privacy policy to reflect this.

Data on the move.
Any personal data that has been provided by a consumer for the use of a contract, or an agreement with the consumer that is automated e.g. a reoccurring subscription, should be easy to move, copy or transfer personal data from one IT environment to another in a secure way without affecting usability. E.g. if your site doesn't already allow a quick download of your clients' account transactions, this will need to be updated.

Profiling your consumers…
The GDPR defines profiling 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". Consumers must be informed of the existence of profiling, for example, when you obtain data about an individual (regardless of whether it is directly from the individual or indirectly from third parties). You MUST provide information about where you got their data from.

The right to say no!
The consumer must freely give consent to have their data collected and processed by you and must be fully informed of what they are consenting to.

In the event of a data breach…
Any data breach where it is likely to result in financial loss, loss of confidentiality, or any other significant disadvantages, should be reported to the ICO and in some cases, to the individuals. You are required to have your site's security regularly checked and updated, this will help to ensure that you don't ever have to tell your customers that their privacy has been breached. It might be worth looking at a company that will do this for you for a monthly fee.

Delegate a Data Protection Officer.
You will need to appoint a Data Protection Officer (DPO) for your business. The person that holds this position will be responsible for your compliance with the GDPR. This position should be given to someone who has been specifically trained to deal with this. Unless you are processing personal data on a massive scale (in which case, consider outsourcing a DPO), a current member of staff should be perfectly sufficient for this role.

Pseudo-What now?
Pseudonimisation is a procedure whereby the identifying fields (e.g. name) within a data record, are replaced by an artificial identifier (e.g. a unique ID). If you are storing identifiable personal data, you should really be working towards pseudonymising your data. This will ensure an extra security measure in case of a data breach, if personal data was stolen, the data wouldn't contain actual names, just extra data. This is quite a large undertaking and will affect your CRM systems, you will need to discuss this with your CRM developers to ensure that they will be compliant in time.

It sounds like a lot of work, what happens if I'm not compliant?
If you don't follow their rules the Information Commissioner's Office (ICO) will start by handing out a warning letter to you. If the letter doesn't make you budge, they'll fine you 4% of your annual turnover. So, it's really in your best interest to become compliant with the new regulation.

So, how can I prepare for this regulation?
Save yourself time and stress. Start preparations now. You'll want to sort out all of your current data, familiarise with where all it is stored and who can access it. Make sure you have a policy and prevention against the risk of a possible security breach on your data. It's important to document everything so you can show the ICO that you're following the new regulation.

Do I have to still pay a fee to the ICO because of the new regulation?
At the minute under the current DPA, you're having to notify them about the personal data you collect and what you do with it. Depending on the size of your business, you may or may not have to pay them a notification fee. Starting from 1st April, and the GDPR is about to come into play, you'll still have to pay them a data protection fee, but there's no requirement to notify them on the information you're collecting. But don't worry if you're a small business, as the new system ensures the fee is fair and reflects the risk of your business when it comes to the processing of data.

If you want to know more about how you should get started, then check out the official guide from the ICO o what you preparation.