What is required under GDPR?

The goal of GDPR is to protect user's personally identifying information (PII) and hold businesses to a higher standard when it comes to how they collect, store, and use this data. The personal data includes: name, emails, physical address, IP address, health information, income, etc.

While the GDPR regulation is 200 pages long, here are the most important pillars that you need to know:

1. **Explicit Consent** – if you're collecting personal data from an EU resident, then you must obtain explicit consent that's specific and unambiguous. In other words, you can't just send unsolicited emails to people who gave you their business card or filled out your website contact form because they DID NOT opt-in for your marketing newsletter (that's called SPAM by the way, and you shouldn't be doing that anyways). For it to be considered explicit consent, you must require a positive opt-in (i.e. no pre-ticked checkbox), contain clear wording (no legalese), and be separate from other terms & conditions.

2. **Rights to Data** – you must inform individuals where, why, and how their data is processed / stored. An individual has the right to download their personal data and an individual also has the right to be forgotten meaning they can ask for their data to be deleted. This will make sure that when you hit Unsubscribe or ask companies to delete your profile, then they actually do that (hmm, go figure). I'm looking at you Zenefits, still waiting for my account to be deleted for 2 years and hoping that you stop sending me spam emails just because I made the mistake of trying out your service.
3. **Breach Notification** – organizations must report certain types of data breaches to relevant authorities within 72 hours, unless the breach is considered harmless and poses no risk to individual data. However, if a breach is high-risk, then the company MUST also inform individuals who're impacted right away. This will hopefully prevent cover-ups like Yahoo that was not revealed until the acquisition.
4. **Data Protection Officers** – if you are a public company or process large amounts of personal information, then you must appoint a data protection officer. Again, this is not required for small businesses. Consult an attorney if you're in doubt.

To put it in plain English, GDPR makes sure that businesses can't go around spamming people by sending emails they didn't ask for. Businesses can't sell people's data without their explicit consent (good luck getting this consent). Businesses have to delete user's account and unsubscribe them from email lists if the user ask you to do that. Businesses have to report data breaches and overall be better about data protection.