Here is 3B Digital’s 28-step action plan to get prepared for GDPR (the eu general data protection regulation).

Find this list online at https://www.3bweb.com/blog/gdpr-compliance

- ❏ Create a **data protection compliance folder** on your company file system. This will form the basis of your proof of compliance.
- ❏ Every step you take towards GDPR compliance should be documented to be used in your defence if necessary.
- ❏ Keep **notes** of internal meetings on GDPR, and decisions made on GDPR
- ❏ Name a **data protection officer**
- ❏ **Map your data**, i.e. establish what data your business collects and where
- ❏ Separate the data into **categories**
- ❏ Identify the **lawful basis** for processing each category of data
- ❏ **Refresh consent** where necessary (and consult with 3rd party data processors like Mailchimp to ensure they have established compliance too!)
- ❏ Implement a policy to identify and handle any **data subject access requests**
- ❏ Implement a policy to identify and handle any **data erasure or corrections requests**
- ❏ Create a document of **non-compliance issues** to show awareness of compliance omissions and to plan towards total compliance or at least thorough risk mitigation.
- ❏ Create a **password policy** for all users (staff, website etc)
- ❏ Contact your entire database (marketing or otherwise) before the 25th May 2018 to ask them to **opt in** to the various types of communication you plan on sending
- ❏ Keep a **record of consents** for those who have already opted-in, and those who are still to do so.
- ❏ Create a **retention schedule** for data. When the data has reached the end of its retention period destroy it in accordance with a **data destruction policy** (minimise the data you hold)
- ❏ Train your staff so they ALL understand **what constitutes personal data** (bonus points for practicing case scenarios with your team and for putting together an **Staff GDPR Awareness Status Report** to note down who has participated in which training)
- ❏ Train your staff to **identify a breach** (plus how to avoid email scams)
- ❏ Have a **breach response policy**
- ❏ Create a **data breach log** to record events such as "Stacey emailed the client list to Tim Smith in the finance team not Tom Smith in the sales team".
- ❏ Ensure your website is **HTTPS** (security by design)
- ❏ Ensure your office **computers are encrypted** (security by design) - Go to Settings > Security & Privacy > FileVault on a Mac to do this.
- ❏ Review the **physical security** of data (USB disks, paper filing systems behind lock and key etc)
- ❏ Create an **asset register** of the serial numbers of all your computers regardless of contents - you may need to prove to the ICO that a stolen computer could not have had any personal data on it
- ❏ Consider which individuals should have **access to the data on each device**
- ❏ Securely **lock away any data**
- ❏ Update your website's **privacy policy** (to include identity of the controller purpose of the processing and the legal basis, the legitimate interest, any recipient or categories of recipients of the personal data, the right to withdraw consent at any time, and the data retention period)

❑ You may also want to get specific and mention **which cookies are on your website,** and give users the option to opt-out. This is HUGE, as it means you'll need to gain opt-in consent before providing a user with a Google Analytics tracking script. You can view the ICO's cookie policy, and you may want to use the Cookie Control tool by Civic UK which we are using on our website too.

❑ Have an **extra pair of eyes** look through what you've done, both technical and legal, in case there are some simple further steps which you need to take before you're fully compliant

❑ If you process data within the UK - consider registering with the ICO (Starting at a £55 annual fee + £20 if you're in the direct marketing industry)

Email support@3bweb.com for any technical questions.