# GDPR Checklist

What you can do to make sure you're prepared for GDPR.

**Update your Definition of 'Personal Data':** ☐

*You need to be aware of the personal nature of new forms of **technical data** such as IP Addresses, Geo-location, Biometric Data, Mobile Device Identifiers and also **social data** such as psychological identity, genetic identity, cultural and social identities and economic status.*

**Figure out how you will handle 'Consent':** ☐

*You need to be able to **prove consent** of the individuals whose data you possess. You need to ensure that you are very clear about what data they are giving over, **how long** it will be used for, **what purposes** it will be used for and **who** will have access to it. At the same time, define 'personal data' to the user.*

**Update and Streamline your User Agreements:** ☐

*As a society, we have a bad habit of not reading user agreements. To be fully GDPR compliant, a **streamlined** and **easy to read** user agreement should be implemented. It should be **shorter and to the point.***

**Determine how you're going to handle Data Requests:** ☐

*GDPR allows users to **request their data** from you in an **electronic format**. You need to be able to comply with this in a **timely** manner*

**Ensure that you have the Proper Protocols:** ☐

*A user can request that their information be **permanently deleted** ('The Right to be Forgotten'), as such you need to have a system in place to handle these requests both **easily** and **timely**.*

**Do you need to hire a Data Protection Officer:** ☐

*Typically, if you are a company that collects and/or processes data then the answer is 'Yes'. You are able to hire an **established employee** to fulfil the role of the **DPO**.*

**Discard old data that is no longer useful:** ☐

*If you're **no longer using** the personal data or elements of that data in providing your services/products then there is **no reason to risk** this in a potential security breach. It's best to always r**emove the data** you're not going to need any more.*

**Figure out what to do in the event of a Data Breach:** ☐

*You need to conduct an assessment on the impact of a data breach on your company. Doing this will help you address any holes that are found in governance initiatives. A contingency plan needs to be in place in the event that a breach occurs, how would you tell the users of the breach and when will you do this?*