FUNNELYTICS

GDPR Compliance Checklist

- [ ] Create a data deleter for customers.
  - This only applies to businesses that handle and collect a significant amount of user data.
  - For businesses that only collect small amounts of data such as an emails, manually deleting data at the request of a customer is sufficient.
  - with the exception of data that may be needed for legal reasons, or tax reasons
  - Must be immediate. (undue delay)
- [ ] Make sure you have the technical capabilities to meet data portability requirements.
- [ ] Create data moving/porting capabilities for customers.
  - Put in CSV format, or at least a readable format that can be moved and used.
- [ ] Determine whether you are a data controller or a data processor.
- [ ] Make sure all future and past agreements between the data controller and processor detail their respective data breach responsibilities.
  - outline communication line between data controller and processor
- [ ] Make sure you have a plan in place to report data breaches within 72 hours to authorities.
- [ ] Write up a thorough incidence response plan. Make sure your data controller/processor has one too, so when it hits the fan, you know what to do.
- [ ] Appoint Data Protection Officer.
  - if there is a data breach, will leakage of data violate risks and freedoms of people's whose data have been leaked? If so, we need a Data Protection Officer.
- [ ] Privacy Notice (Policy)
  - Apply the necessary alterations when changes happen with your product or service so that it remains GDPR compliant.
  - Make sure that it is in concise, complete, and plain language.
  - Know who is in charge of privacy notice (Data Protection Officer), so GDPR compliant changes can be made promptly when needed.
- [ ] Outline the following:
  - What data are you collecting and why.
  - What data are you sharing and why.

- How long are you storing that data for and why.
- Communicate this with customers with clarity

- [ ] Have a security protocol in place to protect data.
- [ ] If you are the data controller, provide a privacy notice and a method of getting consent to handle data.
- [ ] If you're a processor, be sure to take direction from a Controller. Update any necessary agreements pertaining to the Controller.
- [ ] Outline data transfer routes between you and any third parties (processors, vendors, marketing companies, etc). Specify controller and processor relationships.
- [ ] List out all the systems that handle data:
  - Whom are we collecting data from?
  - How are we collecting data?
  - How and where are we storing data?
  - How can we port data?
  - How do we deliver data when requested?
  - How do we delete data when requested?
  - What automated data can be deleted?
- [ ] Have a way to document the personal data that is collected in each system.
- [ ] Get Consent for data collection and handling:
  - Are you able to document consent path?
  - Are you able to manage opt-in opt-out path? (even if user is going back and forth)
  - Are you able to provide evidence that shows opt-in date?
  - Are you able to collect consent from existing users?
  - It cannot be a pre-checked box nor can it be a condition of service. Must be a separate opt-in requirement.
- [ ] Are there any gaps in your security controls?
  - How is your data protected?
  - Who has access to it?
  - What are the gaps in your security?
  - If there are gaps, is a plan in place to remediate them?