Are you GDPR Compliant?

RAISING AWARENESS

- ❏ You've informed all required parties (marketing team, IT, compliance, etc) of the New GDPR policies
- ❏ You've informed key decision makers such as management of the changes

AUDIT YOUR EXISTING DATA

- ❏ You've documented the existing data that you hold (names, where they came from and when you collected it)
- ❏ You've informed any other organizations that you've shared data with if there are any inaccuracies in your data (i.e. if you've shared an old subscriber list with non-consenting individuals)
- ❏ You've properly documented your data in an easy to navigate document should you be required to provide proof of consent

PRIVACY INFORMATION

- ❏ You've updated or sent out a privacy notice clearly indicating who you are, what you're doing with personal data, and the lawful basis on which you are processing data
- ❏ You've indicated the appropriate data retention period in your documentation
- ❏ You've expressed in your notice that individuals have the right to oppose the processing and retention of their personal data to the ICO (Information Commissioner's Office)
- ❏ Your privacy notice and all other existing public documentation are written in an easy to understand and unambiguous language

THE RIGHTS OF INDIVIDUALS

- ❏ You've set in place proper procedures in the event of an individual demanding for erasure of their personal data (it is their right to request so)
- ❏ Your process for erasure requests must be easy to navigate and written in an easy to understand, and unambiguous language

PROCESSING REQUESTS

- ❏ You have the means to process requests from individuals within a 30 day period
- ❏ Should you refuse/charge a request (which you are able to do should the request be unfounded or excessive), you have expressed in your privacy notice and other documentation that individuals have the right to complain to ICO

COMMUNICATIONS

- ❏ You have made it clear in your documentation on which lawful basis you will be processing data
- ❏ You've updated all existing documentation to reflect this decision as you cannot change your basis later on to fit your current needs (i.e switching from basis of consent to basis of legitimate interest to continue processing the personal data of an individual who requested erasure)

CONSENT

- ❏ You've updated all existing data collection processes to include a clear, positive opt-in (unchecked checkbox)
- ❏ You've clearly indicated the measure of an opt-in separate from other terms (i.e written clearly next to the checkbox)
- ❏ You've included a withdrawal mechanism (an unsubscribe button) to all communications and must be clearly indicated (i.e written on its own line on the bottom of an email)
- ❏ You've refreshed and updated all existing lists to include only those who have given expressed consent
- ❏ You've named any third parties who rely on the individual's consent in your documentation, expressed clearly with the positive opt-in
- ❏ You've recorded when an individual consented, what they were told at the time of consent, how they consented (e.g. newsletter subscription, at checkout, etc.) and if they have withdrawn consent (unsubscribed)
- ❏ You've established a double opt-in process for email communications (it's best practice and easier to keep a clean record of consented individuals)
- ❏ You've sent out a re-permission campaign to your list of non-GDPR consenting individuals, or those you are not sure if they have given expressed consent. This will clean and refresh your existing lists.

PARENTAL CONSENT & CHILDREN

- ❏ You've implemented an age verification process for acquiring children's data (e.g.. a date of birth function to a form or sign-up process)
- ❏ Your existing lists have expressed parental consent for children under the age of 16 (can be lowered to 13 in some EU states such as the UK)
- ❏ Your terms are written in a language that children under the age of 16 can understand

PREPARING FOR DATA BREACHES

- ❏ You have the right procedures in place to detect, report and investigate a data breach Should you have a data breach, you have reported it to the authorities within 72 hours

DATA PROTECTION OFFICERS (DPOs)

- ❏ If you are a public authority, organization that monitors individuals on a large scale or work in a sector that collects sensitive data such as medical information, you have appointed a DPO
- ❏ This individual is up-to-date on all GDPR compliance requirements, laws and regulations and takes on sole responsibility should there be a breach or other legal issue