GDPR – SUMMARY – points to remember

Purpose of Act = to protect people from misuse of data

- **IT ALL STARTS WITH AN AUDIT OF YOUR CURRENT POSITION.**
  - **HIGH RISK –** *sensitive / could do harm if breached*
  - **CURRENT PERSONAL DATA HELD –** know why, who, what, when & where?
  - **NEW DATA –** *set up good practice models for May 25th onwards*

✓ **WHY is personal data processed? Why do you need it?**
✓ **WHOSE personal data is processed? List will help map what is needed for each group eg; Staff, Members etc...**
✓ **WHAT personal data is processed? Keep it explicit & limited. Must be able to demonstrate that it is lawful, use one of these five to justify reason for keeping:**

1. **CONSENT – not always needed (see other 4 reasons)**
2. **CONTRACTUAL WITH THE INDIVIDUAL**
3. **LEGITIMATE INTEREST – to fulfil the needs of your organisation**
4. **COMPLIANCE WITH LAW**
5. **A PUBLIC TASK – UK Public Authority**

✓ **WHEN is personal data processed? When will you delete? – need simple opt out (permanent)**
✓ **WHERE is personal data processed? Secure & confidential – who has access?**

REMEMBER -

- **EVIDENCE – document your compliance / show your audit / map the process**
- **SHARE INFORMATION – make sure all of your organisation knows – especially anyone who is "data processing" ie; all who process/handle data**
- **REPORTING BREACHES – Process – Likely to cause risk to an individual = 72hrs – know how to report to ICO**
- **TRUSTEES – make sure they know their responsibility and liability (SHARED)**
- **DATA PROTECTION OFFICER – only need to have one if processing large amounts of personal data regularly**
- **BUT should have named Data Officer & Board Member (you can call them whatever you like eg; GDPR Compliance Lead!!)**

Remember – KISS – Keep It Simple Sam!!

Look at current first & then set new guidelines moving forward.