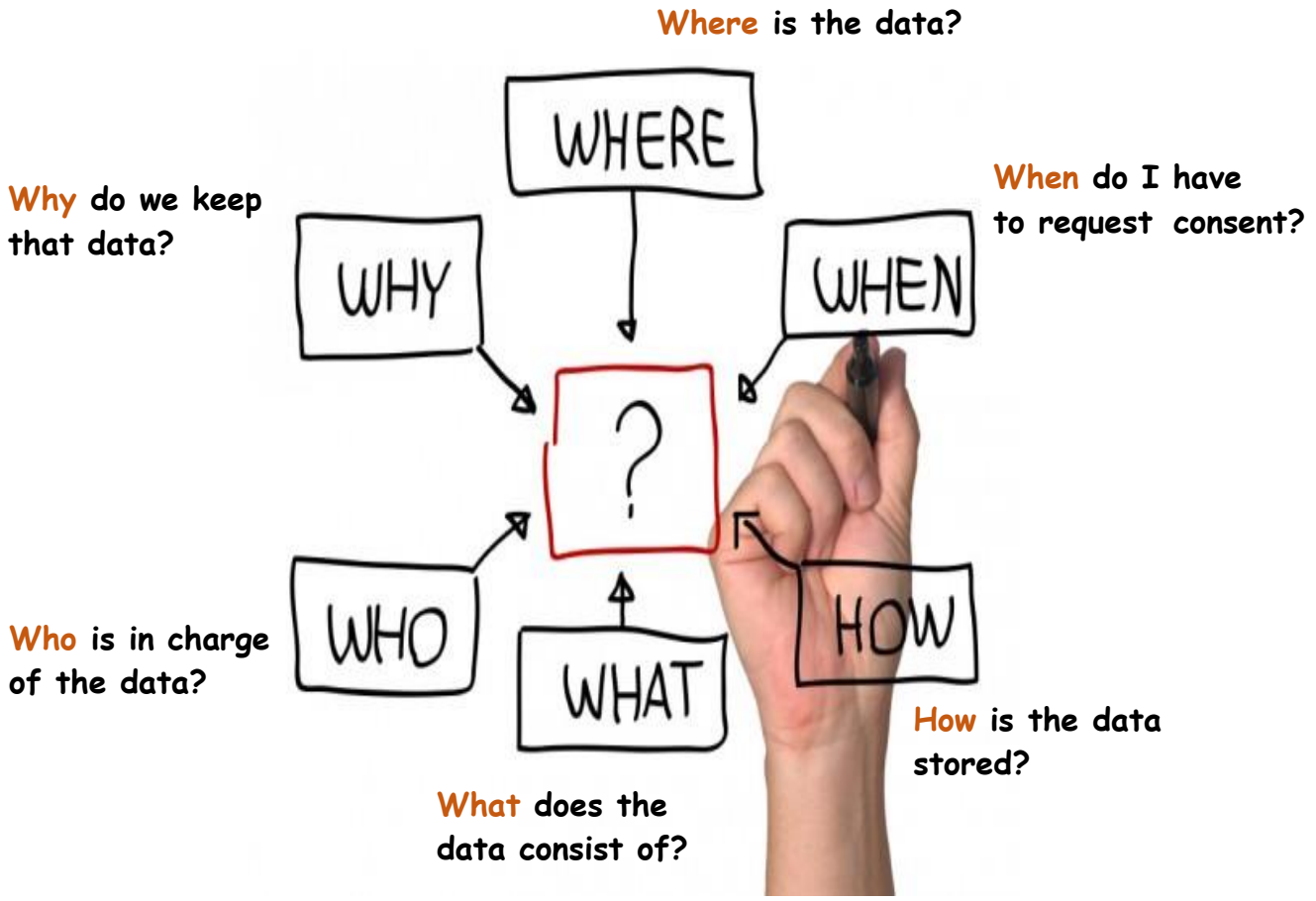
GDPR Handout for Local Community Groups

On the 25th May 2018, a new law called the General Data Protection Regulation (GDPR) came into force that 'tightened' up the previous rules regarding data protection alongside the Data Protection Act 2018 (DPA2018). THE GDPR can't be described in a few lines but one important change resulting from its implementation requires that you give your active consent to how your organisation communicates with its members in the future. Your 'presumed' consent will not suffice. In practice this means that if you are happy to receive information from your organisation on events, meetings, newsletters, offers, marketing and fundraising you need to complete and sign a form, so the organisation has a record of that consent.

It should be stressed that there shouldn't be a change in the amount of information your organisation sends you, so you won't be bombarded; but the organisation must make this change to comply with the new law. Equally important is the right you have, to withdraw your consent at any item in the future, which could be simply done by an email or telephone call, and the withdrawal must be noted and adhered to.

The diagram below shows how your organisation should be viewing the data it holds:



REMEMBER: The data you 'hold' doesn't belong to you – It belongs to the 'data subject' (the person) – you're just keeping it in a safe place and using it for their benefit – (for contacting members about meetings / events / newsletters etc.)

GDPR is specific in the requirements for collecting, storing, processing and retaining personal data. Each of these **topics** necessitates certain characteristics where the data must be:

- **Lawful, fair and transparent** - processed lawfully, fairly and in a transparent manner (e.g. with specific opt in for consent or legitimate interest and 4 other conditions)
- **Purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed. Further processing for archiving purposes in the public interest, scientific or historical research may require anonymisation / pseudonymisation
- **Minimised** - adequate, relevant and limited to what is necessary
- **Accuracy** - accurate and, where necessary, kept up-to-date, having regard to the purposes for which it is processed
- **Storage limitation** - kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- **Integrity and confidentiality** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (includes password protection or encryption)
- **Accountability** - managed responsibly by the Data Controller, (the person who 'keeps the data') who shall be responsible for and be able to demonstrate compliance

These capabilities demonstrate an organisations ability to support the rights of the individual. In addition, the regulation requires organisations to rapidly notify any data breaches (e.g. data loss incidents) to the Information Commissioners Office within 72 hours of a Data Breach.

Data can mean: Name & Address, Email, Telephone Number, date of birth, religion etc.

If you have a membership form, It MUST have a 'consent' statement on it about how their data will be used, stored & shared.

If you are dealing with 'children' then *currently* under 16's need parental approval for consent and if the children are accessing a 'portal' / social media site – the GDPR / New Data Protection Act has dropped the age down to 13 for giving consent, so the wording on the form has to be written in a way which a 13-year-old can read and understand.

Rights of individuals

Under GDPR, individuals have the following rights with respect to their **personal data**:

- to be **informed**
- to have **access**
- to ensure **rectification**
- to ensure **erasure**
- to **restrict processing**
- to **data portability**
- to **object**
- to **understand** and **constrain automated decision making**, including profiling

Your organisation is accountable for the data they hold about you and must take this responsibility seriously – but really, it's common sense.

So, if you aware of GDPR but are not exactly clear what is meant by the terms: Personal Data, Sensitive Data, Data Subject, Data Processor, Data Controller, Data Breach, Pseudonymisation, Purpose Limitation, or what your organisation is supposed to be doing with them, I would suggest you look at the ICO Website (www.ico.org.uk) or contact Richard Newell from **GDPR-Info Ltd** – he'd be happy to tell you more about it.

One final thing – if you're a member of a club – make sure it's registered with the ICO – The current annual registration fee is £35.00.