CJCH CAVEAT

The observations below are intended as informal and generalised expressions of opinion to which no legal duty of care will apply.

They do not constitute formal advice on which any reliance can be placed in any specific context.

Independent formal legal advice ought to be sought from appropriately qualified legal practitioners on any specific issues and concerns.

1. Are there different requirements depending on the size / income of the charity?

- The GDPR is intended to unify data protection legislation, so there aren't many overly specific provisions at this stage
    - Worth noting that the legislation could be subject to change. Brexit isn't going to affect the implementation of the GDPR and the UK Data Protection Bill is already going through Parliament, specific derogations relating to more relevant situations – GDPR allows the UK to legislate in these areas.
- Generally, you might say the risks are higher for organisations that are processing sensitive information, quantity of information and employing more people, harder to keep tight control of what is being shared and individual breaches.
    - Fines are more likely to be (proportionately) higher for larger organisations just by virtue of their size and revenue
- Some myths about who needs to appoint a Data Protection Officer (DPO)
    - Where there are over 250 employees you must appoint a DPO" – FALSE
    - MUST appoint a DPO
        - Where an organisation's core activities include large scale systematic monitoring of data subjects
        - Public authorities
        - Process a large scale of special category data
    - Usefully there has been no definition of large scale so it's open to interpretation at this stage. Many organisations should have someone responsible for data protection but not necessarily require an internal DPO
        - However – relating back to the question, might argue larger organisations are more likely to come under 'large scale"

- Records of processing activities – Article 30 GDPR
    - DOESN'T apply to organisations with fewer than 250 employees (
        - *unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects;*
        - *the processing is not occasional;*
        - *or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.*

2. Is free training and support for implementing available for small charities

If you are obtaining free advice, even if it is from any of the sources below, would be wise to make a note of this so you can document any decisions you made and the fact you sought this advice in the first place

- There are numerous sources that are providing general advice on GDPR
    - Information Commissioner's Office (ICO) – Supervisory authority for data protection in the UK – main source of information relating to data protection, provided FAQs, myth-busting articles
        - Also provided a helpline for small businesses and charities
        - Article for charities on the ICO website but is only offering general advice / FAQs
    - Third Sector - https://www.thirdsector.co.uk/gdpr
        - Provide useful links for charities and third sector organisations including some of those included below
    - Advice for small businesses: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/
    - For charities: https://ico.org.uk/for-organisations/charity/charities-faqs/

3. What is recommended as effective online data protection for a small Charity - (no network, no server, just using a PC & or laptop for admin)? We have - Firewall & Virus/Internet Security protection, - anything else needed?

- Included a link to the ICO guide for security and steps organisations would take
- The measures required are likely to depend on the number of people that are accessing the information and how many machines are going to be storing personal information
- Important to understand your processes, will help assess threats and risks

General points

- Document any decisions you make and why you made them
- Try to make sure you're not using personal machines for work/business
- Separation of files – depends where the information is being stored
    - Try to encrypt files where possible and password protect them
    - Backup – cloud is a useful solution but be aware of where your cloud storage is located (may be outside of the EU)
    - Limit the use of any programs/software that are unnecessary – relates back to avoid using personal machines
    - Use a respected e-mail provider (Outlook/Hotmail) if sending data via e-mail, ensure things like two step authentication is in place
    - Keep software and computers up to date
    - Act on any prompts from virus/malware updates
    - Local security – ensure access is only given to those who require it and be aware of who has access to specific files (if more than one person)
    - Train staff
    - Physical security is important – printing and storage of these files is just as important
        - Make sure anything confidential is shredded or appropriately destroyed
- Government services
    - Get Safe Online - https://www.getsafeonline.org/
    - Cyber Street - https://www.cyberaware.gov.uk/
    - Cyber Essentials - https://www.cyberessentials.ncsc.gov.uk/
- Many points discussed included in the ICO's security - https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

4. A small registered charity with a membership of 40 mostly young people aged 11 to 18 shares details of its members, including name, age address, contact details, parents details and any health issues, with the local authority which also processes this information. They give their consent for the information to be shared. The charity deletes this information once the person leaves the organisation but the local authority retains it for a longer period. Will this arrangement be able to continue after GDPR and what steps should the charity take to ensure it complies with the regulations?

- Children identified under GDPR as 'vulnerable individuals' and requiring 'specific protection'
    - Privacy notices provided to children make sure they are:
        - Concise, transparent and in plain language – "so the child can easily understand"
- Consent isn't always the best way to process personal information, which may seem counter intuitive, in theory, consent is great, but it doesn't work in many scenarios. This is an example where it can work, but there are factors that an organisation needs to be aware of
- You won't be able to rely on 'previous'/'historic' consent unless it matches up to what is set out in the GDPR legislation.
    - Must be freely given, specific and informed, unambiguous – given "by a statement or clear affirmative action"
    - Opt-in NOT opt-out
- Must keep records of consent, where possible for what purposes it was required and review these mechanisms regularly
    - Here where the information is deleted – try and give the person an idea of how long the information is likely to be stored for
- Health data is special category data under the GDPR and must not be processed unless an exception under Article 9 can be applied
- Should inform the person you intend to share it with the local authority but they would need to have their own data protection policy in place
- Where information is removed – be sure that you are in fact removing every instance of the data
- Legitimate interests may be relevant here

5. Can data be used and kept to log enquiries? Is consent required for this?

- Consent may be required, it depends on the nature of the information and the reason for which it is collected/processed
    - If you are collecting enquiries to enter into a contract with someone for example, then you could state that you are processing the information at the request of the data subject for preparation to enter into a contract
- If no other situations are applicable – you must have the person's consent
    - Provide them with a privacy notice, whether this be as part of an online form, state the reason they are giving you the personal information, they consent to its use
        - Telephone enquiries – may be more appropriate to use an online privacy notice and make it available for people – impossible to obtain written consent at this stage – processing at this stage could be based on a legitimate interest (balancing test would be easy to establish as they information is being provided by the data subject)