GDPR

GDPR was at the top of organisations' 'to do' list when the legislation came into force in May 2018, but unfortunately it has slipped down the ladder of priorities somewhat since then. Sobus would urge organisations to make sure you keep on top of this and make sure you are regularly reviewing and updating your policy and practice.

If you're still in a GDPR muddle – don't panic! GDPR requirements seem rather daunting, but in reality, particularly for small organisations, it shouldn't be as overwhelming as it appears. Remember – you didn't have to have everything in place by 25th May, but you should have in place a clear plan on how your organisation will work towards being GDPR compliant.

The following link will take you to the Information Commissioners office (ICO), which has lots of helpful information. https://ico.org.uk/for-organisations/charity/charities-faqs/

In essence, you need to give careful consideration to:

- What personal data you hold (names, addresses, email address, phone number, photos, any further info about the individual)
- The legal basis on which you process this data – for many organisations it's probably "Consent of the data subject", with individuals specifically giving their consent to join your mailing list and receive information from you.
- How it is stored, and how you ensure the data is safe and secure (e.g. is data held on multiple PCs, do your PCs have reasonable anti-virus software etc. Do you keep paper copies of any personal data – if so are these safely stored, or securely destroyed?)
- What it is used for being absolutely explicit about what you use their information for, e.g. we will use your data to send you newsletters, invitations to our events, etc. If you will use the personal data from your mailing list for any other purpose – you must be clear what this might be, e.g. we may use your data to contact you for our fundraising purposes, or we may include your data in our monitoring information to our funders/supporters.
- How it is shared: include how it is shared within your organisation, not just externally, and whether you are likely to use photographs or case studies in your reports, social media or publicity etc.
- Opt in, not opt out: For each purpose or activity that you use people's data for, your membership form should have a clear and explicit opt in function.
- Right to information: your members have right to have a copy of all the personal data you have about them, and to ask that it be corrected if it is wrong
- Right to be forgotten: your members have the right to request that you permanently delete their data from your system

Consent: For many organisations, you will be storing data on the basis of "consent of the data subject" – i.e. you have explicitly asked individuals if you can contact them for specific purposes. Like us, I'm sure you have been inundated with "reply now or be removed from our mailing list forever!" emails. However, the advice we have received suggests that it

isn't necessary to have updated consents from everyone on your mailing lists immediately – but you might want add a covering sentence along the lines of…*You are receiving this because you have signed up to receive our newsletters/or expressed an interest in our services in the past. If you no longer wish to receive this, please call us on xxx or email xxx so we can remove you from our mailing list.*

Don't forget – GDPR applies to everybody. It's not just your service users, but also your staff, volunteers and also any contractors that you might use. You need to be clear with all of these how you hold and use their information, for what purposes and under what legal basis.

If you'd like further information or support around your GDPR policy, please contact Sobus: info@sobus.org.uk