considerations (which ICF partners will also need to follow so you must speak to them about the practical logistics of this):

- Obtaining consent – consent must be active, i.e. a positive indication of an individual's agreement (no pre-ticked boxes, opt-outs or consent by default). If *explicit* consent needs to be obtained (for special category/sensitive personal data) this must be very clear and specific, distinct from any other consents being requested and expressly confirmed in words;
- Consent requests should stand out clearly and prominently, separate from other terms and conditions – consider what works best for the relevant media and isn't overly disruptive to the individual's use of a service (e.g. for online products and services using '*just-in-time*' notices so that relevant information appears at an appropriate time);
- Consent must be granular – if you are processing information for a range of purposes: explain the different ways you will use the information, and provide a clear and simple way for people to indicate that they agree to different types of processing. Don't use blanket consents – people should not be forced to agree to several types of processing simply because e.g. the privacy notice only includes an option to agree or disagree to all; they should be able to consent to their information being used for one purpose but not another. Consider listing the different purposes with separate unticked opt-in boxes for each or Yes/No buttons of equal size and prominence;
- Informed consent, choice and control – give people sufficient information to make an informed choice, which includes identifying yourself (i.e. the ICF Chapter) as the data controller and naming any third parties who will be relying on consent. Avoid using vague or confusing language. Make it clear and obvious that people are being asked to give consent and what they are being asked to consent to. Don't use consent unless people have a genuine choice. Avoid making consent a pre-condition of a service, i.e. where processing the personal data is not necessary for that service[1]. You still need to ensure transparency of processing by including in privacy notices the prescribed information to be provided to data subjects. Example: The following would *not* be fully informed and valid consent: an "*I agree*" box with no supporting information, or, simply telling a person how you're going to use their personal information (without providing them with the ability to agree or not);
- Third parties – if you are asking people to agree to the use of their data by third parties, you should name those parties specifically – if they are not well-known, you might also explain what type of business they are, e.g. market research. An ICF local group/sub-branch is likely to be considered as a third party for these purposes so people will need to be informed that ICF local groups/sub-branches will be processing their personal data and these ICF local groups/sub-branches should be specifically identified;
- Reobtaining consents – consider how you can obtain consent following any changes to your privacy notice, and how individuals can revoke this consent if they do not agree with these changes. Periodically refresh consent requests, as appropriate (ideally at least every two years) – consent does not remain valid indefinitely;

[1] This concept may seem confusing at first sight. The ICO (draft) guidance on consent gives examples of this issue as follows: "An online furniture store requires customers to consent to their details being shared with other homeware stores as part of the checkout process. The store is making consent a condition of sale – but sharing the data with other stores is not necessary for that sale, so consent is not freely given. The store may ask customers to consent to passing their data to named third parties – but must allow them a free choice to opt in or out. The store also requires customers to consent to their details being passed to a third-party courier who will deliver the goods. This is necessary to fulfil the order, so consent can be considered freely given - although it still not be the most appropriate lawful basis."

required to grant access this information – a request must be documented and this information should otherwise be kept offline. If you archive this must still be GDPR compliant (kept secure etc.).

GDPR does not really address the issue of the secure disposal of personal data – there is some (UK) guidance on deletion under the legal regime being replaced by GDPR so it will have to be seen if there will be specific GDPR guidance on this. This UK guidance comes from the UK's data protection regulator the ICO which says the following about deletion (and archiving) which might be used as a yardstick (care should be taken though as not only might this guidance be replaced under GDPR but data protection regulators in other countries may take a different approach):

- "There is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket. Information that is archived, for example, is subject to the same data protection rules as 'live' information, although information that is in effect inert is far less likely to have any unfair or detrimental effect on an individual than live information.
- However, the ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use', and for data protection compliance issues to be 'suspended' provided certain safeguards are in place:
    - information has been deleted with no intention on the part of the data controller to use or access this again, but which may still exist in the electronic ether. For example, it could be waiting to be over-written with other data.
        - this information is no longer live. As such, data protection compliance issues are no longer applicable. (A parallel situation might be a bag of shredded paper waste. Although it may be possible to re-constitute the information from the fragments, this would be extremely difficult and it is unlikely that the organisation would have any intention of doing this.)
    - information that should have been deleted but is in fact still held on a live system because, for technical reasons, it is not possible to delete this information without also deleting other information held in the same batch.
        - in cases like this the organisation holding the information may be prohibited by law from using it in the same way that it might use live information. This could happen if a court has ordered the deletion of information relating to a particular individual but this cannot be done without deleting information about other individuals held in the same batch.

The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible."

What about social media?

Organizations providing social networking opportunities need to comply with data protection obligations under GDPR in the same way as they would for any other personal data processing activity – the primary data protection obligation is to ensure that users of social networking sites receive appropriate notices and provide relevant consents to use of their data obtained through the site, not only to make use of the site/social network, but also use of data for separate ancillary purposes such as marketing and behavioural advertising. But social networking organizations may not be as compliant as they should be so take care not to get entangled in their possible non-compliance. Also take special care if considering using social networking sites for pre-employment vetting as this might be seen as unfair or discriminatory.

In the context of direct marketing on social media, where, e.g. LinkedIn is used, suggested best practices would be as follows:
Make it clear that you are contacting people in their professional capacity; explain to people why you are approaching them; only directly contact people regarding products/services that are relevant to their role; if you want people to sign up to receive marketing content/news/updates via the ICF Chapter LinkedIn page, they will need to opt-in; and, do not contact them again if they indicate they do not wish for you to do so or ignore your approach. Where Twitter/Facebook/Instagram/ Google/YouTube or new technology, is to be used to target or profile individuals for marketing, do a Data Protection Impact Assessment *first*; note that GDPR introduces data subject rights concerning profiling so these will need to be considered. If new technology is to be used to capture personal data, or different processing activities are to be carried out, do a Data Protection Impact Assessment *before* proceeding. This will help to identify and mitigate any potential risks and will also assist your ICF Chapter's compliance processes.

What do we do if there is a data breach?

As mentioned above, under GDPR there are a number of very important principles that apply to data processing. One of these is called "integrity and confidentiality" – this means making sure that data is processed in a manner that ensures the appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, so ensure that you use appropriate technical or organisational measures.

If there is a failure to ensure data security that will likely constitute a data breach. A data breach is defined under GDPR as follows:

> *"'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;"*

As can be seen, the scope of a data breach is very wide. So, as a rule of thumb consider therefore that a situation that you are dealing with which exposes (or could expose) personal data could constitute a breach – in case you are in doubt in a given situation you may need to seek advice although your first next best step is to report the data breach internally; under GDPR data breaches have to reported to a regulator within 72 hours and, depending on the circumstances, the individuals affected by the data breach may also need to be informed about the breach. A summary of the suggested procedure to be followed has been set out in the "*Key GDPR Best Practices for Chapter Leaders & Members*" document – Chapter Leaders will need to determine how they implement the suggested procedure.