GDPR Basics for ICF Chapters

What is GDPR?

In the EU (28 Member States) personal data can only be gathered under strict conditions and for legitimate purposes only – those who collect and manage individuals’ personal information must protect it from misuse and must respect certain rights. The rules that regulate this are also referred to as “data protection” or “privacy” rules. The existing EU regime has been significantly upgraded under what is called the EU General Data Protection Regulation (commonly referred to as “GDPR”), which comes into full effect on 25 May 2018. Notably, organizations that breach these rules potentially face major sanctions including large fines and affected individuals may also seek compensation from the offending organizations. If you are handling personal data, it is therefore imperative that you comply with GDPR.

What personal data can we collect and how?

**Personal data and data processing**

It is worth setting out the full GDPR definition of “personal data” in order to appreciate its broad sweep, which is as follows:

> “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

As can be seen the scope of “personal data” is of very wide scope (it is wider than e.g. the US definition of “Personally Identifiable Information” often referred to as “PII”). As a rule of thumb therefore consider that any information that relates to an identified or identifiable individual that you are dealing with as personal data, e.g. an email address, a telephone number, personally-identifying credential details etc – in case you are in doubt in a given situation seek advice.

GDPR also has a specific category of personal data which is referred to as “special category personal data”, although many commonly refer to this as “sensitive personal data” (which is its name under the regime that GDPR is replacing). GDPR defines this as:

> “[...] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, [...] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [...]”.

Due to its sensitive nature, a higher standard applies to dealings with this type of data under GDPR, so take extra-special care if you are dealing with this type of personal data.
It is also important to bear in mind that technically-speaking what you are doing with personal data is called “data processing”. It is also worth setting out the full GDPR definition of “data processing” in order to appreciate its broad sweep, which as follows:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

As can be seen the scope of processing is also very wide. So, as a rule of thumb consider therefore that any personal data that you and your ICF Chapter are dealing with, constitutes data processing – in case you are in doubt in a given situation seek advice.

The Chapter Membership Database/Event Database therefore contains personal data that is being processed in a number of ways. There is no limit as such on the type of personal data that can be kept in the database. But, under GDPR there are a number of very important principles that apply to data processing including what is called “data minimisation”. What this boils down to is making sure that the use of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed. As a rule of thumb therefore only keep the personal data in the database (and elsewhere) that you really need.

Consent

As mentioned above, under GDPR there are a number of very important principles that apply to data processing. One of these is that personal data must be processed “lawfully”. This means that dealing with an individual’s personal data can only be done if one of the lawful grounds for processing under GDPR applies. In many cases the most common lawful basis for processing personal data that we will be relying on will be “consent”; without wishing to ignore the other lawful grounds, in the interests of keeping this note short these are not explored here – it is also best to seek advice about these.

The GDPR definition of consent is as follows:

“‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”

As mentioned above, higher standards apply to special category/sensitive personal data under GDPR including the fact that to be able to process this type of personal data explicit consent is required, other than in very specific, narrow situations (which you should seek advice about if you wish to try and rely on any of these). GDPR does not define explicit consent. A commonsense approach is that explicit consent must be exactly that, i.e. an indication of agreement to a statement that consent is given e.g. a tick in a box, or a signature.

GDPR and some of the regulatory guidance that has come out about consent further elaborate on consent requirements – in terms of the practical implementation that ICF Chapters will need to address when dealing with personal data e.g. when acquiring new members, doing marketing, events and training (including taking and posting picture and recording and posting videos) the following are key
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.”
• Recording consents – you must keep a record of consents that lists who consented, when, how and a copy of the exact consent request;
• Withdrawing consent – individuals have the right to withdraw consent at any time and you must make them aware of this. Make it easy for people to withdraw consent and explain how to do this, e.g. preference management tools and opt-out by reply to every contact. Mention the right to withdraw consent in privacy notices. The withdrawal should be an easily accessible one-step process, if possible using the same method by which consent was given;
• Direct marketing – if you are asking people to consent to receive direct marketing, in addition to GDPR, you must consider the obligations under laws relating to direct marketing (this area is governed by separate rules to GDPR, which are being updated to be in line with GDPR). If you want individuals to consent to direct marketing, have a separate unticked opt-in box for this, prominently displayed – you must not send marketing mail to anyone who objects or opts out. You must be granular about informing people what they are consenting to receive by way of marketing materials and through what channels they will receive materials e.g. by email, text etc. You cannot send marketing mail if e.g. an email address was originally collected for an entirely different purpose;
• Marketing events – where badges are scanned at marketing events check/ensure that consent has been obtained to do this for the purposes of direct marketing and that the individuals being scanned have a choice to opt out. Where prize draws are undertaken, ensure people know you will use their details for the purposes of direct marketing and have a choice to opt out/not participate.

These considerations must be built into an appropriate mechanism (such as a form or through a website etc.) appropriate and adapted to whatever the occasion/function is used to obtain etc. personal data (acquiring new members, signing up to training). Addressing consent requirements covers the personal data of whoever you are dealing with, including individuals who are customers of an ICF Chapter’s product and services but not members of ICF Global, as relevant to the basis on which you will be processing their personal data e.g. to meet the requirements for direct marketing.

How long can we store personal data for?

As mentioned above, under GDPR there are a number of very important principles that apply to data processing. One of these is called “storage limitation” – GDPR only defines this in very basic and general terms stating that data mustn’t be kept for longer than necessary. As a rule of thumb therefore consider keeping personal data for shorter rather than longer periods (and the shorter the better) – this will also help reduce risk. This is a judgment call for you to make – one idea to consider would be to draw up a data retention protocol/schedule that sets out periods for how long certain personal data will be kept after which it will be destroyed – some information may need to be held for different periods of time compared to other types of information; certain technology also exists that can destroy personal data at a certain date. If one simple overall retention period can’t be determined for all the information, as part of a rolling data retention/destruction plan the information could be divided up and a table created listing in one column the type of data and in the other column the retention period that has been decided. But you will also need to ensure that you comply with other rules that oblige certain personal data to be kept, e.g. for tax purposes – these rules vary from jurisdiction to jurisdiction and would have to be checked individually.
When determining in general how long to retain personal data the following general check-list should be considered and the elements documented:

- The value of the personal data being retained, both in the future and at the current date;
- The purpose(s) for which the personal data was obtained and the nature of the personal data;
- What the costs, risks and liabilities are that are associated with retaining the information;
- How easy it is to ensure that the personal data is kept up to date and accurate; and,
- If there are any legal or regulatory requirements that may apply.

Sharing personal data within the organization

Sharing personal data within your ICF Chapter may entail risks. As a starting point, data should only be shared if it is necessary to do so. You shouldn’t share personal data about someone which is excessive, i.e. only share a piece of data if it is necessary for your purposes. A key way to minimize risk is to put in place access protocols or controls, using technology where possible – restricting access will also need to be monitored. You will need to continue to assess whether it is still appropriate to be sharing data—it is not a one-off assessment to be made at the beginning of the process and instead it should be undertaken regularly. Consider whether an individual or group of individuals might be negatively impacted by the sharing and whether they might object to what you are doing – might trust in ICF and your ICF Chapter be undermined? Is there a contingency plan for situations when something does go wrong? Can the personal data be anonymized? If so it will then need to be done thoroughly to ensure that it cannot be reversed and used to identify individuals, e.g. by combining with other pieces of information. Make sure that data can be shared securely – it may be necessary to consider using encryption.

You must take an especially high standard of care with special category/sensitive data – this must be restricted to only those individuals with a true need to know. The sharing of special category/sensitive information should be regularly evaluated regarding any possible risks to your ICF Chapter members and those whose personal data ICF is dealing with and how the risks could be reduced. You should regularly create a procedure to discontinue use/storage of old, outdated sensitive information. If relevant a Data Protection Impact Assessment might need to be undertaken e.g. if a new technology is going to be used.

How can we dispose of personal data securely?

As a general principle clearly when personal data is no longer necessary (and probably following a review) it should be securely deleted, including any back-up, unless there is another reason for keeping it, in which case it may be archived.

Consider using secure deletion software but take care and check this as the product/service may not be as secure as is claimed or it may have limits, e.g. it may be ineffective on some media such as write-once CDs; also consider using automated systems which delete data after a certain period where a number of records of the same type of data is held. Or, consider hiring a third-party service provider to delete securely but do your due diligence on the party and the service they offer. For hard copy personal data use secure shredding and disposal systems – also consider using a third-party service provider.

When archiving, the information may be kept for long periods provided that the information is only stored in backup, is very difficult to get at and can only be looked at or retrieved for some very good reason. By way of best practice the authority of a senior figure such as a Chapter Leader should be
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.