Key GDPR Best Practices for ICF Coaches

This document is aimed at providing information in summary form about the data protection principles, people's rights over their personal data, and some key points about data breaches. It is by no means exhaustive of all aspects of GDPR or all GDPR issues nor does this information constitute legal advice, which you may need to seek independently. Reliance on regulatory guidance referred to in this document is at your own choice – please also note that some of the regulatory guidance referred to may be subject to change and some of the guidance was also issued under the data protection regime that pre-dates GDPR.

What do I need to do?

When you handle personal data, you must abide by a number of principles and respect certain rights that an individual has concerning their personal data. These will help you comply with the EU General Data Protection Regulation (GDPR, found here).

What is personal data?
Personal data is any information relating to a person. Technically-speaking, when you handle personal data you are processing it which means almost any operation performed on it including its collection, recording, organization, alteration, transmission and destruction.

Six key Data Protection Principles are at the heart of all data processing and interlink with each other:

1. *Lawfulness, Fairness and Transparency:* You must make sure any personal data is processed lawfully, fairly and transparently. In practice this means that you must:
    a. tell individuals about how you intend to use their data, which you must inform them about when you collect their data
    b. handle individuals' data only in ways they would reasonably expect;
    c. make sure you do not do anything unlawful with individuals' data;
    d. have legitimate grounds for collecting and using personal data.
    The most common way of doing this but not the only one) is to obtain an individual's consent. Consent means an individual's freely given, specific, informed and unambiguous indication of their wishes by which that person, by a statement or some form of clear affirmative action, agrees to the processing of their personal data (so pre-ticked boxes, opt-outs or consent by default are not permitted).
    If you ask individuals to agree to the use of their data by third parties you must also say who those parties are. And, you must keep a record of consents, noting who consented, when, how and a copy of the exact consent request. Individuals must be told that they can withdraw their consent at any time, and it must be as easy for them to withdraw consent as it is for them to give it (for EU regulatory guidance about consent please see here, and for UK regulatory guidance about consent please see here);

2. *Purpose limitation:* You can only collect personal data for specified, explicit and legitimate purposes. You must not process data in a way that is incompatible with those purposes. You need to be clear with individuals about the purpose(s) for which you hold their personal data so that you can then ensure that you process the data in a way that is compatible with your original purpose(s);
3. *Data minimisation:* You must make sure your use of personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) for which you process data. In practice you should identify the

minimum amount of personal data you need to properly fulfil your purpose. You should not hold more personal data than you need. Nor should the data you hold include irrelevant details;

4. *Accuracy:* Make sure that your data is accurate and, where necessary, kept up to date. In practice this means**:** taking reasonable steps to ensure the accuracy of any personal data you obtain; ensuring that the source of any personal data is clear; carefully considering any challenges made by an individual to the accuracy of information; and, considering whether it is necessary to update the information;
5. *Storage limitation:* You mustn't keep data for longer than necessary. In practice this means: reviewing the length of time you keep personal data; considering the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it; securely deleting information that is no longer needed for this purpose or these purposes; and updating, archiving or securely deleting information if it goes out of date (for UK regulatory guidance about deleting personal data please see here). Generally-speaking it is for you to decide how long you will keep data, but please be aware that most countries have separate rules about certain personal data that must be kept for certain periods of time, e.g. with regard to tax records;
6. *Integrity and Confidentiality:* You must make sure personal data is processed securely including protection against unauthorised or unlawful data processing and against accidental loss, destruction or damage. In short, make sure that you use appropriate technical or organisational measures. In practice, this means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You need to design and organise your security to fit the nature of the data you hold and the harm that may result from a security breach. You also need to make sure you have the right physical and technical security, backed up by robust policies and procedures and be ready to respond to any breach of security swiftly and effectively. There is no "one size fits all" solution to information security. The security measures that are appropriate for you will depend on your circumstances, so you should adopt a risk-based approach to deciding what level of security you need (for UK regulatory guidance about security please see here);

You also need to know about:

Data Breaches- Generally speaking a data breach is any data security issue which exposes (or could expose) personal data. If there is a data breach (or a suspected one) it must be reported to a data protection regulator within 72 hours of you first having become aware of the breach. In the event of a data breach it is recommended that your key objectives are to:

1. prevent the further spread/loss of data; recover the data that has been lost;
2. identity risks arising from the breach;
3. contact appropriate parties – in addition to notifying a regulator you may also need to inform the individuals who have been affected of the breach (you may need to obtain legal advice about all of this);
4. and, prevent future breaches.

It is recommended that you record the details of the breach. Also ensure that you act quickly with regard to all aspects of handling a data breach (for EU regulatory guidance about data breach notification please see here);

Data Subject Rights- You must tell people about the rights they may exercise with regard to their personal data, which are as follows:

a. Subject Rights Access – this means that an individual can seek to obtain confirmation as to whether or not personal data concerning them is being processed by you, where and for what purpose, and to be provided with a copy of that personal data free of charge – out of all of the rights this is the one you would be the most likely to be subject to (for UK regulatory guidance about Subject Access Requests please see here);

b. The Right to be Forgotten (data erasure) – this means that an individual can seek to have personal data that you hold on them erased, subject to certain conditions such as the data no longer being relevant to original purposes for processing, or where an individual has withdrawn their consent to processing that data – this is also a right that you might likely be subject to;

c. The Right to Rectification – this means that an individual can seek to have personal data that you hold on them corrected without undue delay where the data concerning them is inaccurate;

d. The Right to Restriction – this means that an individual can seek to restrict you processing the personal data you hold on them, subject to certain conditions such as where the individual contests the accuracy of the data you hold on them for a period enabling you to verify the accuracy of the data in question;

e. The Right to Object to Processing – An individual can object to processing personal data that you hold on them where certain conditions apply which are so-called "legitimate interests" (i.e. not consent), including profiling. Where you process personal data for direct marketing purposes, the individual also has the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. This is a particularly complex right. Please also note that under separate EU rules that sit alongside GDPR, individuals can object to direct marketing by a particular channel e.g. email or telephone; please also note that ensuring that consent has been properly obtained for direct marketing is also very important. Please also note that an individual can also seek to "not be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" – this is also a particularly complex right (for EU regulatory guidance about Automated Individual Decision-Making and Profiling see here);

f. The Right to Portability – this means that an individual can receive the personal data concerning them which they have previously provided to you in a "structured, commonly used and machine-readable format" and have that data transmitted to someone else, subject to certain conditions such as where the individual consented to you processing their data. This is a particularly complex right (for EU regulatory guidance about the Right to Portability see here);

g. The Right to Lodge a Complaint with a Data Protection Regulator – this means that an individual can make a complaint before a regulator about data protection issues concerning them. If this happened it would quite likely because an individual is not satisfied with the way you have dealt with their rights request.

All of these rights are all potentially complex (various conditions apply to them and some are subject to exceptions), so it is recommended you consider seeking legal advice if someone attempts to exercise one of these rights against you.