GDPR Guidance for Members

Note, this document is only guidance and should not be relied upon as the basis for determining the actions that you should or should not take to become fully compliant with the new regulations. If you are in any doubt about how GDPR may affect you, seek expert advice.

What is GDPR?

In recent years, there have been a number of significant issues with personal data:

- Inappropriate use of personal data, most notably where people are sent unsolicited marketing mails (also known as 'spam');
- Serious leaks of data, where people's personal information has been compromised, resulting in fraud related to identity theft.

This is not just a UK issue, it is a global one. As a consequence, the General Data Protection Regulation 2016 (GDPR) will become law in all EU member states, which includes the UK, on **25 May 2018**. This regulation will be assimilated into UK law after Brexit.

GDPR is intended to secure more transparency for data subjects and aims to improve consumer trust. Note, GDPR does not replace the Data Protection Act (DPA), it is introducing new regulations to strengthen the DPA in some key areas. In considering GDPR it is worth remembering some of the current Data Protection Principles, specifically:

Principle 3 – personal information must be adequate, relevant and not excessive.
Principle 4 – personal information must be accurate and up to date.
Principle 5 – personal information must not be kept for longer than necessary.

Please see the Information Commissioners Office web site for more information (https://ico.org.uk) where there are a range of useful resources for both GDPR and the DPA.

GDPR brings with it considerably tighter controls over the processing of data, how data can be used, the rights of individuals on whom data is processed and significantly greater financial penalties for in appropriate use of data, or not protecting data from hacking.

Data is defined as any information that is held in an organised filing system – so this could be a database or an Excel spreadsheet, as examples. Email is considered to be an organised filing system. GDPR tightens regulations around Personal Identifiable Information (PII), which is any data that can be used to identify a person. This might include items such as passport numbers, National Insurance Numbers, Address or Date of Birth etc. It is also worth noting that where combinations of data might lead to the identification of an individual, the regulations also apply. For example, if there is only one Doctor in a village, using the title Dr with the village name is sufficient to identify the person. For the first time, GDPR also expands regulation to cover images and pictures.

What does GDPR mean for me?

If you work as a coach, mentor or coach supervisor in an organisation, then your organisation should be taking steps to ensure GDPR compliance. You may wish to check what your organisation's plans are and how they might specifically impact you.

However, if you deliver these services either via your own limited company or on a sole trader basis, then there are a number of steps that you must take in order to ensure that you are compliant with GDPR when it come into effect. Generally, organisations that are fully compliant with the current Data Protection Act are likely to be compliant with GDPR, but should still ensure that they have addressed all of the requirements that GDPR will introduce.

As mentioned above, the ICO's web site (https:\\ico.org.uk) contains a lot of helpful information about GDPR and the steps that organisations should take. The following suggested 10 step approach below is based upon their guidance.

It should be noted that there are exceptions to the provisions in the GDPR. For example, organisations are required to maintain financial records that must be available for HMRC review for up to seven years. In these instances, the legal requirement to retain these records takes precedence – for example a membership organisation may keep records of member subscription payments (as EMCC UK does) that include name address and Bank details. In such instances organisations should ensure that this data is available for scrutiny by the relevant authorities if required, whilst ensuring the information is only accessible to the people who 'need to access it'.

There may be other regulatory requirements to retain information – such as proof of identity for Anti-Money Laundering obligations.

If you have any questions or concerns about data you may need to hold after the formal relationship with an individual has ceased and their data is to be deleted, seek expert advice.

There is a summary of the key elements of GDPR that you need to consider, at the end of this document. **Please note, this guidance document has been prepared from the perspective of an organisation based solely in the UK.**

Social Media

This guidance does not cover social media. Users of social media create their own accounts (such as on LinkedIn or Facebook) and generally self-manage their membership of any groups that they participate in. Consequently the relevant social media provider needs to address any GDPR considerations. If you have any queries in this respect, please refer to the privacy policies and GDPR statements of any social media providers that you may use. If you have any concerns about GDPR and social media you should seek expert advice.

Step	Theme	Possible action for business owners	Possible actions for members working in organisations
1	**Awareness** Making sure that all the key people in your organisation are aware that the law is changing.	You should make sure that you understand the implications for GDPR on your business. In addition, you should ensure that anyone who you employ or sub-contract are aware that the law is changing and are also aware of any impact upon them.	You should ensure that you are clear on your organisation's plans for GDPR and how they might apply to you in your work.
2	**Information You Hold** You should document the personal data that you hold, where it came from and who you share it with. You may need to undertake an information audit.	Get a full understanding of all personal data (PII as referenced above) that your organisation holds. Organisations may hold personal data on customers, users and staff. Hence all areas of the organisation should be audited. Remember the current DPA principles as set out above, when auditing your data. **It is really important, as part of the audit, to determine who has access to the data and if this is necessary for them to undertake their role or not. If people have access to data that is unnecessary, take the necessary steps to remove the access.**	Read your organisation's guidance on the handling of personal data following the implementation of GDPR.
3	**Communicating Privacy Information** You should review your current privacy notices and put a plan in place for making	As well as amending and reviewing privacy notices and policies (don't forget web sites), consider preparing documents that explain the data and why you need it. It is important to	Ensure you understand your organisation's privacy policies and ensure you adhere to them.

	any necessary changes in time for GDPR implementation.	remember to consider your data retention policies at the same time.	
Step	**Theme**	**Possible action for business owners**	**Possible actions for members working in organisations**
4	**Individual Rights** You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.	A key element of GDPR is the "**right to be forgotten**". Should an individual tell you that they no longer wish you to hold their data, this should be permanently deleted. Care will need to be taken that any back-up copies of data are also amended. **If you share data with third parties, this information needs to be deleted AT THE SAME TIME.** As mentioned above, you may need to keep some data for other purposes – such as details of financial transactions, payments etc. that contain individual information. This can be validly retained where there is a legal or regulatory requirement for you to do so, subject to suitable access control and security that protects the data. We recommend that your privacy policy sets out what data you will retain in these situations, and for how long, for absolute clarity.	This is the responsibility of your organisation.
5	**Subject Access Requests** These are where individuals ask you to clarify what data you hold on them. Under GDPR, timescales for responding to these requests have been shortened. Previously individuals could be charged a fee for this	You should ensure that you have processes and procedures in place that cover how you will handle such requests within the required timescales.	This is the responsibility of your organisation.

	activity, GDPR now requires that Subject Access Requests are free to individuals.		

Step	Theme	Possible action for business owners	Possible actions for members working in organisations
6	**Lawful basis for processing personal data** You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	This complements point 3 – you should create a clear 'customer facing' explanation on the data you hold and what you need to do with it. **This should clearly set out EVERYTHING you will do with personal data. This should be clear at the point where the personal data is obtained. Ensure you DO NOT use the data for any other purpose.**	This is the responsibility of your organisation.
7	**Consent** You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. **This is a really key element of GDPR.**	Consent should be signed and dated, noting that GDPR requires consent to be specific. **There is a new principle of 'opt in', so unless you have clear consent, the default is that the person has 'opted out' of their data being used.** Vague consent is no longer acceptable under GDPR. Consent has to be specific to the activity. For example, if a school has consent to send regular email updates about a child to their parents, the school **must not** include any further information in the mail unrelated to the subject 'regular email update about my child' or they breach GDPR requirements. If you are not fully sure you have consent from the data owner for any personal data that you	Be aware of the consents that are in place for any PII that you have access to and ensure that you do not use the data for any other purpose.

		are using, **either** get the requisite consent **or** STOP USING IT **before the 25th May 2018**.	

Step	Theme	Possible action for business owners	Possible actions for members working in organisations
8	**Children** You should start thinking about whether you need to put systems in place to verify individuals ages and to obtain parental or guardian consent for any data processing activity.	If your work involves working with people under the age of 18, seek further specialist advice. There are specific GDPR requirements in place for children and you need to ensure that you are fully comply with them. These changes are particularly aimed at social media.	This is the responsibility of your organisation.
9	**Data Breaches** You should make sure that you have the right procedures in place to detect, report and investigate a personal data breach.	GDPR requires that any data breaches are reported within 72 hours of personal data being compromised. You should think about how the personal data you hold might be compromised and how you might respond accordingly. For systems that are publically accessible (web sites or IT systems) there are the obvious risks of 'hacking'. However, data may also be compromised if it is held on a laptop or memory stick and these are lost or stolen. Consequently, consider using encryption or other methods of keeping personal data safe, including physical controls (e.g. locking up portable media). **If you share personal information with third parties, get a written confirmation of the steps they take to protect this data.** Note, you are not expected to validate their statement as the ICO acknowledges that many organisations will not have the knowledge or ability to do so. Also, ensure that you have full contact details of any of the organisations you deal with in this respect and that they have yours.	This is the responsibility of your organisation.

Step	Theme	Possible action for business owners	Possible actions for members working in organisations
10	**Data Protection by Design and Data Protection Impact Assessments**	Consider the data that you hold and the harm that might result if this data were to enter the public domain. This then informs any further action that might be necessary. Where you share personal data with a third party, you might want to undertake a Personal Impact Assessment to help with this process. When doing this, remember to consider how you might implement the 'right to be forgotten' with these organisations e.g. when someone asks for their data to be deleted it should be deleted on your systems and third party systems at the same time.	This is the responsibility of your organisation.

GDPR Summary

The key elements of GDPR that are identified above can be summarised as follows:

You need Consent to hold any personal data that you hold and must ensure that the data you seek is proportionate to the need as set out in the DPA (see the comments on DPA principles 3-5 above). You need to explain what you will do with this data and this explanation must be a fundamental part of seeking consent. **Do not use the data for any other purpose other than that which has been consented to**.

In thinking about GDPR, there are some simple questions you can ask yourself:

- What personal (or PII) data do I hold? What do I use the data for? Is the data appropriate to the need?
- How is this data stored so that it is secure, not at risk of being stolen and do I have processes and procedures in place to ensure that personal data cannot be accidentally modified or deleted (a current Data Protection Act requirement). How long do I need to hold it for?
- Do I have the data owners' permission to use it in the way that I do? Consent may need to be more than a single 'tick' box as you may need separate permissions for different types of communication. For example permission to email a person a newsletter does not imply permission to send them marketing messages. Consent statements should be short and simple, so it is clear what the person is signing up to. Long complex and 'bundled' requests for consent will not be accepted by the regulator.
- What do I need to do if there is a data breach involving PII?

Remember the right to privacy and the right to be forgotten. Ensure that processes and procedures require data holders to 'opt in' with the default being 'opted out'. Also have processes and procedures in place to immediately delete personal data at the request of the data owner.

If you do not have consent, do not use the data after the 25th May 2018.

Ensure you have processes and procedures in place to deal with any data breaches within 72 hours.