EU General Data Protection Regulation Frequently Asked Questions (FAQ)

The following are designed to aid members navigating the GDPR and were compiled based on queries received from practitioners. They are not legal advice and every practitioner must satisfy themselves regarding compliance with the GDPR.

No	Question	Answer
1.	What are the key pieces of data protection legislation	EU Data Protection Regulation 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN The Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
2.	List of useful resources	**European Data Protection Board** https://edpb.europa.eu/edpb_en Irish Data Protection Commission https://www.dataprotection.ie/
3.	I'm updating current clients of the practice's GDPR obligations. Do I need to notify both active and inactive clients? Is there any particular time period before which I do not need to notify clients?	The GDPR applies to the processing of personal data. You need to consider the obligations in relation to the personal data you currently process. Processing includes 'storage', so regardless of whether a client is an active client or not, GDPR obligations apply, if you hold a client's personal data. How you decide to notify the customers is a business decision, however care must be taken to ensure that such notification complies with the principles of processing (Article 5 GDPR).
4.	Article 30 Record of Processing Activities – what detail do I need to include and can I use one spreadsheet for	There is currently no guidance from the European Data Protection Board (EDPB) on Article 30.

	all client and employee data?	In considering how to comply with this provision, consideration should be given to whether you are adding to the personal data you hold on a person and also increasing a risk by collating certain data. In terms of the detail required 'categories of personal data', while we are not aware of specific guidance on this, it would seem prudent to keep this high level detail for example "financial data, contract details…" Article 30 does not state that it requires additional detail than categories of personal data.
4.	What is a practice's lawful purpose for processing data that it receives from a client as part of a representation?	The GDPR recognises six lawful bases for processing personal data. While it is possible that a practice's processing may be based on any one of the six bases, in many of the situations in which a practice is retained and must process data, the processing will likely be based upon the legitimate interest of the practice in carrying out its function of representing, advising, or defending clients
5.	Data Protection Officer (DPO): Can you please confirm that it is ok to appoint the same person as data protection officer and data protection representative?	See EDPB guidance on DPO appointment: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 A DPO and an EU Data Representative are two separate and distinct roles. AN EU Data Representative is only required where an organisation is processing personal data that comes within the scope of the GDPR, but does not have a company/office in the EU.
6.	Can a partner in a law firm be the DPO?	A DPO should be independent and not someone making daily decisions on processing data, so a partner is unlikely to be able to fulfil that independent role. A DPO can be an employee or a consultant See DPO guidance from the EDPB http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
7.	What procedure should my practice follow in relation to archived and closed files in order to be in compliance with the GDPR.	Personal data must not be kept for longer than is necessary. It is best practice to have a date retention/deletion policy in place, to include client and non-client data. Data subjects are entitled to know the duration in which you will retain their personal data.

		See Law Society Guidance on data retention and destruction of paper and electronic files.
8.	We are reviewing the office policy in respect of GDPR. In respect of retaining files what is the position in respect of e-files on the case management system. Do we need to delete these after the relevant mandatory period for retention e.g. 6 years for Probate as they will contain personal data?	The GDPR relates to all personal data, and the definition of personal data includes information stored digitally or in a paper form. Personal data can be kept for no longer than is necessary. It is best practice to have a data retention/deletion policy in place, to include non-client data. Data subjects are entitled to know the duration in which you will retain their personal data.
9.	Where a practice is closing, when should the files (including personal data) be deleted?	Files including personal data should be deleted in line with the practice's retention policy and should not be retained after the statutory period expires.
10.	Are data subject rights (right of access and right of deletion) absolute?	Data subject rights are not absolute. Care should be taken in considering the exemptions. The GDPR together with the Irish Data Protection Act 2018 need to be reviewed.
11.	What do I do if my practice discovers a data breach?	Please see EDPB guidance https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 Please see Data Protection Commission website Consideration will need to be immediately given to managing the breach and complying with the practice's notification obligations.