Annexes to GDPR Guide for Barristers and Chambers

ANNEX 1

What you should do next

AUDIT, ASSESS, IMPLEMENT, DOCUMENT

AUDIT

What data am I processing – obtaining, storing, disclosing etc.?

Where am I storing it?

Who do I disclose it to?

Who do I get it from?

What data processors do I use?

What contracts do I have with them?

How do I dispose of data?

ASSESS

Does my processing comply with the DPA/GDPR?

This is question of the gap between actual processing and compliance.

You can use this guide to help you decide.

IMPLEMENT

How do I ensure that my processing does comply?

What lawfulness basis can I rely on?

Do I need to keep all this data?

What do I need to change?

Do I need help to do this and who can help me?

DOCUMENT

I need to be able to prove that I do comply.

I need records of all my agreements - policy documents e.g. data retention policy, privacy notices, any decisions I make about

how I am processing the data- e.g. reasons for not answering a SAR or where I decide that notification is disproportionate.

The ICO has prepared a 12 step document which you should consider using to assist you in ensuring you are GDPR compliant (Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now and a questionnaire which may assist with the **AUDIT**.

It would be sensible to set aside some time, as soon as possible to start this and discuss with your Chambers, if appropriate, how you are going to implement any changes.

ANNEX 2

Checklist of Some of the Points to Consider[1]

1. Written policy on Information Security
2. Contracts between members and chambers
3. Contracts with service providers (including chambers IT support)
4. Password security
5. Use of encrypted and unencrypted email
6. Encryption – particularly for laptops, tablets, smartphones, portable storage devices, and cloud storage folders
7. Check the physical security of your home, car and office and the location of any servers
8. Sharing tablets, computers and other devices with other persons (e.g. family members)
9. Use of personally-owned devices by pupils and staff, including deletion of data when they leave chambers.
10. Policy on home-working for staff
11. Backups, including reliability of synchronised folders
12. Check the geographical location of any offsite storage, including Cloud servers.
13. Cross-border transfers
14. Data retention policy/deletion of old files and emails
15. Disposal of redundant equipment (computers and including hard disk drives)
16. Obtaining references for new staff
17. Periodic audit of facilities, equipment and procedures
18. Consideration of need for a Data Protection Officer and carrying out a Data Protection Impact Assessment

[1] This is not exhaustive and some matters may not apply to you while other issues may apply to you which are not shown.

19. Handling of hard copy papers
20. Use of fax
21. Periodic training of barristers and staff in relation to information security and compliance with GDPR

ANNEX 3

Extracts from GDPR Recitals and Article 29 Working Party Guidelines on Data Protection Officers and Data Protection Impact Assessments

Click here to access the material of the Article 29 Working Party.

"**Core activities**":

> "Article 37(1)(b) and (c) of the GDPR refers to the 'core activities of the controller or processor'. Recital 97 specifies that the core activities of a controller relate to 'primary activities and do not relate to the processing of personal data as ancillary activities'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.
>
> However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs. …
>
> On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity."

"**Large scale**":

> Recital 91: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by

an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

"… it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop for identifying in more specific and/or quantitative terms what constitutes 'large scale' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.

In any event, the Art. 29 WP recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

<u>Examples of large-scale processing include:</u>

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)

- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer"