wiggin

Retention Principle

In this video I'm going to talk about the Storage Limitation Principle under the GDPR, which is probably best known as the Retention Principle. The wording of the principle states that *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.* Or, to put it more succinctly, personal data should only be kept for so long as is necessary.

No doubt many of you will have faced questions regarding preparing and implementing a Retention Policy for your company. That is to say, preparing a policy which sets out how long personal data of various data subjects will be retained. This is a simple ask in theory but far harder in practice.

The first point to note here is that each controller is able to define for itself what is meant by "necessary". Now this doesn't mean that a company can simply define "necessary" as forever and ignore its retention obligations, but it does mean that each company is able to set its own retention periods relevant to its business provided that these are justifiable.

When trying to determine retention periods, companies may consider the following:

- Any legislation requiring it to hold information for a certain period of time or any legislation requiring it to delete information after a certain period of time
- Any relevant industry standards or codes of practice
- The purposes for which the personal data is processed
- Whether the data can be kept without any identifying information, and thus anonymising the data
- If there are any claims relating to the individual where the personal data may be required for bringing or defending such claim

These reasons should all be factored into setting a retention practice. Of course, the commercial benefit to the company can also be considered but this should be weighed against the previously mentioned considerations and against the expectations of the relevant data subjects.

It's also important to note that the ICO would expect companies to go further than simply having a single retention period for all personal data. Now whilst it is wholly impractical to review each piece of personal data individually on a daily basis to determine if it should be retained, a company should be looking to categorise types of data and data subject. For example, staff data and customer data may well require differing retention periods. A more recent example of specific retention periods relates to COVID information – where companies may have been required to test staff and positive results should be retained for an appropriate period but no longer, such as 14 days.

Setting a retention policy and complying with the retention principle are vital for all companies to do. Looking at the data held and understanding any legal retention requirements, processing purposes, likely expectations and commercial benefits are all relevant when arriving at a suitable time period for retaining personal data.