

## Patients Know Best Data Controllership Assessment

**Author:** Kaleidoscope Consultants

**Date:** September 2017

The following assessment uses the [guidance](#) issued by the Information Commissioner's Office to determine the responsibility of Patients Know Best under s 1 (1) of the Data Protection Act 1998 (Art.4(7) of General Data Protection Regulations 2016) which determine which organisation is the Data Controller.

**Who exercise's overall control over the 'why' and 'how' of a data processing activity?**

PKB have a predetermined corporate mission;

(to ensure that patients know best through)

1. Owning a copy of all health information about them
2. Understanding what this information means
3. Using this understanding to make a shared decision with family and professionals

This 'why' factor is realised through partnering with healthcare providers to facilitate such a service for patients.

PKB have determined the information it will require to deliver the service prior to engagement with any third party, such as integration methods and architecture of the portal. Its service is designed and operated for the patient but enhanced through partnership with healthcare partners. Patients are required to sign up to the Terms of Service / Privacy Policy of PKB. - **See ICO Example 1 below.**

- The product had been developed prior to engagement with current client and this includes scoping the information that would be required and the legal gateway to do so.
- The Terms of Service were drafted prior to engagement with any third party.
- PKB has a degree of freedom in respect to the processors they use and who they partner with to deliver their service.
- The portal is their own intellectual property and PKB could withdraw the service from the partners and continue to hold the data for patients – **See ICO Example 2**

<p><b>Who decides to collect the personal data in the first place and the legal basis for doing so?</b></p>	<p>The portal had been developed prior to engagement with any third party and this includes scoping the information that would be required and the legal gateway to do so.</p> <p>The Terms and Conditions of collection were drafted prior to engagement with any third party.</p> <p>Providers will likely be processing data on the lawful basis of medical purposes. The patient effectively makes the independent decision for PKB to collect the data and PKB will be processing on a distinct lawful basis - consent which they collect and record independently.</p>
<p><b>Which items of personal data to collect, i.e. the content of the data;</b></p>	<p>The PKB portal had been developed prior to engagement with any third party and this includes scoping the information that would be required and the legal gateway to do so.</p>
<p><b>The purpose or purposes the data are to be used for.</b></p>	<p>The PKB mission effectively determines the purposes for the data, prior to engagement with any third party. PKB have drafted their Terms of Service prior to engagement with any third party and also have creative control of the future of the technology and therefore what the data might be used for in the future (within the legal framework).</p>
<p><b>Which individuals to collect data about.</b></p>	<p>PKB are effectively able to make decisions about the geographical focus of their business, as with any organisation but the decision about who will use the service is made by the patient themselves. PKB will make decisions about how the information is presented and how the portal will work. <b>See ICO Example 3</b></p>
<p><b>Whether to disclose the data, and if so, who to.</b></p>	<p>Essentially, the decision on whether to disclose the data to other providers of care / relatives rests with the patient who may exercise this control within the PKB service. This relationship and decision is distinct from the relationship with the commissioning provider.</p> <p>If a patient wishes to provide record access to an out of area hospital, this will be facilitated by PKB without requiring any additional permissions from the commissioning provider.</p>
<p><b>How long to retain the data or whether to make non-routine amendments to the data.</b></p>	<p>Both parties have agreed what the data will be used for but PKB, as the party drafting the terms and conditions for the portal have creative control of the future of the technology and therefore how long the data is retained and what data might be included in the future (within the legal framework)</p>
<p><b>Conclusion</b></p>	<p>PKB is a Data Controller by virtue of;</p> <ul style="list-style-type: none"> <li>• Direct contractual relationship with the patient</li> <li>• Distinct lawful basis for processing</li> <li>• Ability to retain data beyond a relationship with commissioner / provider</li> <li>• Ability to share data beyond commissioner / provider with consent from patient</li> </ul>

- Freedom to develop services / product
- Distinct Terms of Service

## ICO Example 1

### *“Payment services*

*An online retailer works in co-operation with a third-party payment company to process customers’ transactions. The payment company is not the retailer’s data processor, even though there is a contract in place between the two companies that covers areas such as service standards and financial arrangements. This is because the payment company:*

- *decides which information it needs from customers in order to process their payments correctly;*
- *exercises control over the other purposes the customer’s data is used for, for example direct marketing;*
- *has legal requirements of its own to meet, for example relating to the use and retention of payment card data; and*
- *has its own terms and conditions that apply directly to the retailer’s customer.*

## ICO Example 2

### *“IT services*

*A car hire company contracts a vehicle-tracking company to install devices in its cars and monitor them so that cars can be recovered if they go missing. They specify that the tracking company should track all the company’s cars and send back the location data to the hire company six hours after the end of the hire period, if the car has not been returned.*

*However, despite these instructions, the vehicle-tracking company is a data controller in its own right. This is because it has sufficient freedom to use its expertise to decide which information to collect about cars (and their drivers) and how to analyse this. It is entirely in control of its own data collection – **the operation of the vehicle-tracking software is a trade secret** and the hire company does not even know what information is collected. Although the hire company determines the overall purpose of the tracking (the recovery of its cars), the fact that the tracking company has such a **degree of freedom to decide which information to collect and how**, means it is a data controller in its own right.”*

### ICO Example 3

#### *Market research company*

*“A bank contracts a market research company to carry out some research. The bank’s brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the UK. The bank leaves it to the research company to determine sample sizes, interview methods and presentation of results.*

*The research company is processing personal data on the bank’s behalf, but it is also determining the information that is collected (what to ask the bank’s customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means that the market research company is a data controller in its own right in respect of the processing of personal data done to carry out the survey, **even though the bank retains overall control of the data in terms of commissioning the research** and determining the purpose the data will be used for.”*