Guidance Note

Dealing with personal data

(In the form of a Q & A)

Q: I am a NED of a Fund and/or Management Company, do I need to register in my own right with the ODPA?

A: If you are a NED of an entity that is registered with the ODPA then, so long as the personal data you deal with is in relation to discharging your duties to that entity and the business of that entity, you will be covered by that entity's registration with the ODPA. However, you must ensure you process and hold that personal data in accordance with the privacy notice issued by the entity and adhere to its policies and procedures in relation to the treatment of personal data. In that regard you should check that your contract/letter of appointment with the entity adequately covers data and personal data including access to that data while you remain on the board and after you have left the board.

Otherwise, if you use personal data (as described above) **for your own business purposes** then you will need to register with the ODPA in your own right.

Q: I retain personal data of my business contacts (e.g. "*Rolodex*"), do I need to register with the ODPA?

A: Yes. As a NED you may also receive other personal data (other than your business contact list) that you use for business purposes not related to the entity where you sit on the board.

Q: I retain personal data of my friends, newsagent, milkman, gardener, decorator, Christmas list etc., do I need to register with the ODPA?

A: No. There is a carve out for personal data that is used for "domestic and household" purposes.

Q: How do I register with the ODPA?

A: You can register with the ODPA on line through its website (https://odpa.gg/)

Q: What will be the fee to register with the ODPA?

A: The fee is £50 paid annually.

Q: How do I know if I am a "Controller" or "Processor" of personal data?

A: Where you do anything with personal data (including simply holding it) then you are processing data and, unless either of the following exceptions apply, you will be either a Controller or Processor and be required to comply with the data protection regime.

Where you process that data solely for the purpose of your personal, family or household affairs then the data protection law does not apply to you.

Where you process that data **only** as part of your contract of service with the Fund / Management Company then the processing is done by the Fund / Management Company. However if you processed that personal data other than exclusively in relation to the provision of services to the Fund/Management company then you would fall to be an controller in your own right.

Q: What is a "Controller"?

A: A person (individual or legal) that, alone or jointly with others, determines the purposes and means of the processing of any personal data. If you exercise overall control of the purpose and means of processing personal data – i.e. you decide what data to process and why – you are a controller.

The responsibilities of a controller can be found on the ODPA Website (https://odpa.gg/).

Q: What is a "Processor"?

A: An individual or other person that processes personal data on behalf of a controller and includes a secondary processor (another processor engaged by the primary processor). Processing is limited in scope and if you have decision making power in relation to the purpose and means of the processing then you will be a controller rather than a processor. If you do not have any purpose of your own for processing the data and you only act on another's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data.

The responsibilities of a processor can be found on the ODPA Website (https://odpa.gg/).

Q: Is a Fund or a Manager that outsources all of its functions to a third party administrator a Controller or a Processor?

A: The Fund or the Manager that outsources all of its functions will be a Controller and, depending on the scope of the discretion given under the agreement, the third party administrator will either be a Processor or a joint controller as regards the personal data passed over. *The administrator can be both a Processor and a Controller as it will deal with personal data in its own right. Where an administrator has employees then it will be both a Controller in relation to that employee data and, potentially, a processor in relation to the data passed to it by clients.*

Given the above, it will be the board of the Fund or Manager that will then have to meet with the obligations of being a Controller.

Q: What is, and what is not, "Personal Data"?

A: "Personal data" has a very broad legal definition, it is: **"any information relating to an identified or identifiable [living] individual"**. Personal data is information that relates to an identified or identifiable living individuals, i.e. their personal information.

Personal data includes both facts and opinions about the individual, as well as information regarding the intentions of the data controller towards the individual. For personal data to be caught by the data protection law, it must either be processed electronically or, where held in manual records, those manual records must be searchable according to a specific criteria. For example,

miscellaneous papers thrown into a draw with no structure are not caught whereas a desk rolodex would be caught..

Examples of personal data include:

- Your address
- Your email
- Your browsing history
- Your car registration
- What your boss wrote in an HR file about you
- Your social security number
- **Any other information related to you**

Special Category Data
Within the overarching term "personal data" there is a sub-category called "special category data" – this is a specific list of types of data that need **extra protection** because of the harms that may result if this data is mis-used:

- Racial or ethnic origin
- Political opinion
- Religious Beliefs or similar
- Trade union membership
- Physical or mental health wellbeing
- Sexual life
- Criminal proceedings
- Convictions
- Genetics
- Biometrics

Personal data does not include:

- ✓ any data about a **dead person**
- ✓ any information, facts or opinions **that do not relate to or identify people** (e.g. employment statistics, or anything else that has been irreversibly anonymised). However, where the information is apparently anonymised but the reader has information that allows him/her to identify the individuals then it will be personal data (e.g. the document just refers to a senior manager but the reader has information that allows him/her to know who that senior manager is).

Q: If I have registered in my own right as a NED, what protocols do I need to put in place?

A: There are a number of things you need to do:

1. Prepare your privacy notice. This must include certain statutory information including:
    - Your identity and contact details
    - What personal data you will hold and if any is special category data
    - The source of the personal data
    - The purposes for which that personal data will be used and on what grounds you are allowed to use it
    - The recipients, or categories of recipient, to whom you will/may pass that personal data as well as a statement about where they are located and

(depending on where the recipient is located) the safeguards applying to the transfer
- How long that personal data will be held
- A statement of the individuals rights in relation to the data including his/her right to complain to the data protection authority.

2. Document the key aspects of how you will hold and process the personal data in your control including data security, what you would do on discovering a data breach and your retention period.

Q: What are the consequences of my not registering in my own right?

A: Failure to register when required to do so is a criminal offence under the data protection legislation and is potentially punishable by a fine or imprisonment.

If you do not register and a data breach occurs where you implicated, then it may be determined that you have failed to adhere to a legal requirement. The ramifications of NEDS not complying with the law by not registering when they should have will be taken into account in any enforcement action, but the nature of the data breach and the culpability of the NED in that regard will likely determine the level of any resultant sanctions, financial or otherwise.

Q: What happens after I retire as a NED?

A: If you cease all business entirely then it is likely that any personal contacts you retain would fall into the category of domestic and household use and, in that case, you would not need to register with the ODPA but you should continue to hold the data securely and securely destroy it when no longer needed. If however you are still conducting business and using personal data in that regard, even if you are not a NED, you will need to register with the ODPA.

Disclaimer: This information is for guidance purposes only and should not be regarded as a substitute for taking the appropriate professional advice

Reviewed: Q421