JERSEY DATA PROTECTION/GDPR ISSUES
INITIAL BOARD CHECKLIST
DATA CONTROLLERS IN A FUNDS CONTEXT

CAREY OLSEN

Introduction

Jersey data protection law (both the existing Data Protection (Jersey) Law 2005 and the new legislation coming into force on 25 May 2018 – the Data Protection (Jersey) Law 2018 (the **"DPJL**")) applies to data '**controllers**' and '**processors**'.

A **data controller** determines the purposes and means of processing personal data. In a funds context, General Partners of fund entities and Listed Fund Entities are typically likely to be **data controllers.**

A **processor** is responsible for processing personal data on behalf of a controller. Typically, an administrator (and other service providers will be a **processor.**

Other functionaries in a funds context are likely to be processors – but may be controllers in their own right. A full data protection audit should be undertaken to assess each functionary.

A fund services provider acting as a data processor may also act as a data controller in respect of certain activities where it does determine the purposes and the means of processing. The most obvious example of this is where a data processor has its own regulatory obligations which require it to carry out its own anti-money laundering checks.

If you are a **processor**, data protection places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

However, if you are a **controller**, you are not relieved of your obligations where a processor is involved – the GDPR/DPJL places further obligations on you to ensure your contracts with processors comply with the GDPR/DPJL.

Controllers and **processors** which are **established in Jersey** will be subject to **Jersey data protection law**. The DPJL also applies to controllers and processors **not established** in Jersey:

- who use equipment in Jersey for processing the data otherwise than for the purposes of transit through Jersey; or
- whose processing is for the purpose of offering goods or services to persons in Jersey or monitoring the behaviour of such persons.

The **EU General Data Protection Regulation** (the "**GDPR**") applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU – so it will often have effect in Jersey.

Please note that this checklist is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such.

This Document

This document is intended to act as an agenda for an initial board discussion within a Fund entity (or General Partner) in order:

- to assess the current status of the Fund as regards data protection.
- to identify the key steps which need to be undertaken to achieve compliance.
- to apportion responsibility and agree action points for compliance

Key Areas	Comments	Action Points
1. Structure and Service Providers		
1.1. You should ensure that you have an up to date structure chart which identifies: 1.1.1. Relevant jurisdictions 1.1.2. Controllers 1.1.3. Processors/service providers 1.1.4. Advisors (eg accountants/legal advisors etc) 1.2. You should ensure that you have identified and obtained copies of agreements with service providers and advisors entered into by the Fund. 1.3. You should ensure that you have obtained and considered copies of any offering documents or subscription		

Key Areas	Comments	Action Points
agreements issued (or used) by the Fund.		
2. Lawfulness, Fairness & Transparency		
2.1. You should ensure that the Fund conducts an **information audit** in order to: 2.1.1. Map personal data flows 2.1.2. Document: a. What personal data you **hold** b. Where it was **obtained** from c. Who you **share** it with d. What you **do with it** e. Who it is **disclosed** to		
2.2. You should ensure that you: a. Have reviewed the purposes of your processing activities, and selected the most appropriate lawful basis (or bases) for each activity. b. Have checked that the		

Key Areas	Comments	Action Points
processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose. c. Have documented your our decision on which lawful basis applies to help in demonstrating compliance. d. Have included information about both the purposes of the processing and the lawful basis for the processing in your privacy notice. e. Have also identified a condition for any special category data which you process, and have documented this. f. You have also identified a condition for processing any criminal record data which		

Key Areas	Comments	Action Points
you process and have documented this.		
2.3. You should review how you ask for and record any **consent**[1] which you rely on and that where you are asking for consent you ensure that: a. You keep your consent requests separate from other terms and conditions. b. Consents are collected via a process of positive opt-in. Use unticked opt-in boxes or similar active opt-in methods. c. You avoid making consent a precondition of service. d. You are specific and granular in your consent process - allow individuals to consent separately to different types of processing wherever appropriate.		

[1] Note that consent is generally difficult to rely upon and other lawful bases shoud be considered if available.

Key Areas	Comments	Action Points
e. You name the Fund and any specific third party organisations who will rely on this consent. f. You keep records of what an individual has consented to, including what you told them, and when and how they consented. g. You tell individuals they can withdraw consent at any time and how to do this.		
3. INDIVIDUAL RIGHTS OF DATA SUBJECTS		
3.1. You should ensure that the Fund provides appropriate **privacy notices** to data subjects.		
3.2. You should ensure that the Fund has appropriate **processes and procedures** in place to deal with the following **individual rights**:		

Key Areas	Comments	Action Points
a. Rights of **access to personal data** and to other information b. Right to **rectification** and to ensure **data quality** c. Right to **restrict processing** d. Right to **erasure** (including a **retention and disposal policy** to routinely and securely dispose of personal data that is no longer required in line with agreed timescales as stated within your contract with the data controller.) e. Right of **data portability** f. **objection** to the **processing** of their personal data g. Rights related to **automated decision making including profiling**		

Key Areas	Comments	Action Points
4. ACCOUNTABILITY & GOVERNANCE		
4.1. You should appoint a **data protection lead** or a formal **Data Protection Officer.**		
4.2. The Fund must have in place appropriate: 4.2.1. **Data protection policies** 4.2.2. An ongoing **monitoring programme** to review and update: a. data protection policies b. the effectiveness of data handling and security controls 4.2.3. **Risk assessment** policies and procedures in relation to personal data related risks 4.2.4. **Data protection impact assessment** processes 4.2.5. **Appropriate technical and organisational measures** to: a. implement **data protection**		

Key Areas	Comments	Action Points
by design and **default** into your processing activities b. Ensure the **security of personal data** 4.2.6. **Board oversight policies** in relation to data protection issues		
4.3. You must ensure that the Fund has effective and documented process to **identify, report, manage and resolve any personal data breaches**.		
4.4. You must ensure that the Board reviews all **data processing arrangements** within your organisation to ensure that: 4.4.1. you have **written agreements in place** 4.4.2. the **written agreements** comply with the **requirements** imposed by the **GDPR/DPJL**		
4.5. You must ensure that you have reviewed		

Key Areas	Comments	Action Points
all prospectus, offering documents or subscription agreements issued by the Fund for data protection purposes.		
4.6. Under the **GDPR**, if the Fund is located outside the EU, and you offer products and services to citizens in the EU, then there is a requirement for you to appoint (in writing) a **representative** within the European Union[2].		
4.7. Where you transfer personal data outside the European Economic Area (which includes for these purposes Jersey and Guernsey), the Fund must ensure an **adequate level of protection** for that personal data**.**		
5. Notification		
5.1. Under the Data Protection (Jersey) Law		

[2] Note – following Brexit, a representative within the UK will no longer be sufficient.

Key Areas	Comments	Action Points
2018, controllers and processors will need to register and pay a fee in relation to processing. There are transitional arrangements meaning that the current £50 per year fee will continue to apply until 25 May 2019.		