Contents

Introduction 01
Governance and Accountability 02
Third Party Management 03
Privacy Framework 04
Monitoring and Reporting 05
Our Team 06
Introduction

Deloitte understands the challenges in the financial sector and the standards expected by regulators. With extensive experience and subject matter expertise in data protection and regulatory compliance, we stand ready to support investment funds in meeting their data protection obligations.

Our Team
Deloitte’s privacy compliance team is passionate about the financial services industry and dedicated to providing pragmatic privacy compliance solutions tailored for the specific requirements and compliance obligations of investment funds.

Incorporating best practices and tested solutions developed from our Regulatory and Data Privacy Services teams, our compliance service is geared to assist investment funds to meet regulatory compliance challenges, while maintaining continual success in an increasingly competitive market.

GDPR for Funds
Overview
The EU General Data Protection Regulation (GDPR) represented a move towards a new privacy culture in an increasingly digital era. Initial efforts to achieve a baseline compliance to the regulation have given way to the implementation of overarching privacy governance models.

GDPR compliance frameworks are best driven by solid data governance, marked by awareness, control, and oversight of personal data collection, processing, storage, and transfers. Entities that process personal data must focus on embedding a governance framework in their organisation that supports both ongoing compliance with the regulatory obligations, as well as effective oversight of data protection risks.

The Challenge
When it comes to investment funds the GDPR poses unique challenges. While the processing of investor personal data is typically performed by delegates of the Fund, the Fund’s Board or Management Company will nonetheless be responsible for GDPR oversight of its delegates, including all data processors.

Further, whether domiciled in Ireland or elsewhere, Funds serviced in Ireland are widely distributed throughout the EU. Data is processed in Ireland (by the Transfer Agent) and sometimes by other parties outside Ireland, depending on the operating and distribution models of the Fund. With issues such as regulatory accountability, outsourcing, vendor management and cross-border data transfers the ongoing monitoring of GDPR obligations for investment funds can be complex.

Our GDPR Fund Solutions
Deloitte’s GDPR Fund Assist Programme helps Fund and Management Company Boards manage their ongoing data protection obligations by establishing a framework within which the Board can oversee its delegates and manage privacy risk in a real and sustainable way.

Deloitte’s Programme is provided by a team of Privacy and Regulatory specialists with extensive subject matter expertise and experience, dedicated to providing support and solutions for investment funds in maintaining GDPR compliance.
Governance and Accountability

Overview
Data protection governance is the building block for an organisation’s approach to their personal data processing activities. It is the bedrock of the organisation’s overall data protection strategy and ensures that accountability mechanisms are in place at all times. As investment funds look to a long-term compliance strategy for the GDPR, a well-developed governance structure is essential to ensure that delegates and service providers process personal data in line with GDPR obligations and ultimately the Fund’s data protection strategy.

Our Services
Deloitte’s Governance and Accountability Service for Funds provides our clients with the experience and expertise to design and drive the Fund’s governance and accountability strategy. A core element to this service is that we work with the client to ensure that the overall structure is based on the client’s own risk appetite while also ensuring compliance.

Deliverables include:
- Report detailing gaps in the Fund Data Protection Governance framework
- Indicative Governance Structure

“Compliance with the GDPR is now a Board level responsibility, and firms must be able to produce evidence to demonstrate the steps that they have taken to comply. The requirement to treat customers fairly is also central to both data protection law and the current financial services regulatory framework.”

UK FCA and ICO, Joint Statement – February

We can assist our clients by utilising the Deloitte governance assessment tool and best practice approach, specific to investment funds, to support the following objectives:

Assess
Our Service begins with establishing the as-is by:
- reviewing the Fund’s current state of GDPR compliance to quickly and immediately pinpoint any key risk areas
- determining whether the key data processing risks for the Fund have been considered in line with the Fund’s own operating model
- assessing the adequacy of the interaction between the Fund Board/Fund DPO/Privacy teams within the Fund’s delegates

Create
We offer our clients off-the-shelf and tailored governance frameworks that:
- establish a clear structure and purpose for the Fund’s GDPR Compliance Programme
- assist the Fund’s Board or Management Company in establishing a GDPR compliance oversight structure for delegates and service providers
- determine whether a DPO or data protection lead at Fund management level is required
Third Party Risk Management

Overview
Organisations often do not realise the full extent and scope of the third parties they have engaged. In the investment fund world, this can get even more challenging when we take the nature of the relationships with third parties into consideration. This coupled with the potential use of many sub-processors can lead to scenarios where the Fund does not have full visibility over their third party landscape and cannot ensure that all third parties and sub-parties are adequately vetted and monitored. Under the GDPR data processors can be held liable, however, there remains an onus on data controllers to ensure adequate controls are in place.

Our Services
Our team will assist the Fund with this particular challenge in order to determine whether adequate consideration is given to the responsibilities of the Fund as Data Controller, and the relationships between the Fund and joint controllers or data processors and sub-processors (including relationships outside EEA).

Deloitte’s Third Party Risk Management Framework for Funds:
Our privacy and fund specialists work with our clients to build their target operating model for third party management including:

- Third Party Policy development and implementation
- Creation of due diligence processes
- Controls testing for third parties
- Reporting models

Example of a typical Third Party Risk Management Framework
Privacy Framework Management

Overview
The risks of non-compliance, and struggles in demonstrating adherence to GDPR accountability mechanisms, can often be attributed to a lack of an effective privacy policy framework. A solid privacy framework for an investment fund should drive programme implementation across Fund delegates and service providers, and embed processes for handling personal data of investors at all levels.

Our Services
Deloitte’s professionals will support the Fund in developing and managing an overarching privacy governance framework, geared for ensuring that investor personal data is protected, governed, managed and utilised effectively.

- Assess
  - Perform a Privacy Risk Assessment to determine the appropriate privacy framework for the Fund

- Design
  - Develop privacy policies for the Fund which document and guide the implementation of the GDPR compliance framework
  - Support the Fund in the creation of a best practice GDPR compliance strategy

- Implement
  - Support the implementation of the Privacy Policy across the Fund network (operationalising requirements and embedding procedures to ensure they become business as usual)

- Operate
  - Develop processes for maintaining data inventories and data lifecycles for the Fund, including the capture of the legal basis for the types of personal data processing agreements, if necessary

Having a clear strategy ensures that personal data is protected, governed, managed and utilised effectively. In order to build an effective privacy framework, our experts believe it is of utmost importance to identify the needs of the organisation:

- Align to the organisation’s privacy governance and strategy
- Consider the organisation’s external responsibilities to their data subjects
- Effectively implementing internally drives employee awareness and ensures compliance and operational excellence
Monitoring and Reporting

Overview
Building an effective privacy framework that encapsulates all elements from governance right through to monitoring and reporting can prove challenging. Organisations often overlook or de-prioritise the task of on-going monitoring and reporting. For the investment fund industry this is a crucial step which gives the Fund the oversight and control that it needs as a data controller and assures and attests to compliance at all times.

Our Services
Our team will work with the Fund to design, build and embed a monitoring and reporting methodology to include a target operating model of on-going compliance through an embedded and effective structure.

Our GDPR Compliance Monitoring and Reporting Management Service provides clients with:

- Establishment of a methodology to carry out GDPR compliance reviews of the Fund’s direct obligations to include:
  - Procedures for obtaining an annual compliance statement from each in-scope delegate or service provider
  - Creation and implementation of data subject rights monitoring processes
  - Attestation procedures for data retention compliance
  - Build and implement oversight procedures for ensuring the adequate implementation of technical and organisational measures by delegates and service providers
  - Support the implementation of breach reporting processes and post-breach analysis

A typical Fund relationship map
Our team

Laura Wadding
Partner – Regulatory Risk
lwadding@deloitte.ie
+353 1 417 2934

Donal Murray
Director – Data Privacy Services
donmurray@deloitte.ie
+353 1 417 8587

Nicola Flannery
Senior Manager – Data Privacy Services
niflannery@deloitte.ie
+353 1 417 2665

Steve O’Donovan
Manager – Regulatory Risk
stodonovan@deloitte.com
+353 1 417 2717

Rachael Gallagher
Manager – Data Privacy Services
ragallagher@deloitte.ie
+353 1 417 2250

Colum Roche
Manager – Risk Advisory
coroche@deloitte.ie
+353 1 417 2280

Annamarie O’Beirne
Manager – Regulatory Risk
aobeirne@deloitte.ie
+353 (0)1 417 2242
At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 286,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte Ireland LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC1499 and its registered office at 19 Bedford Street, Belfast BT2 7EJ, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2019 Deloitte Ireland LLP. All rights reserved.