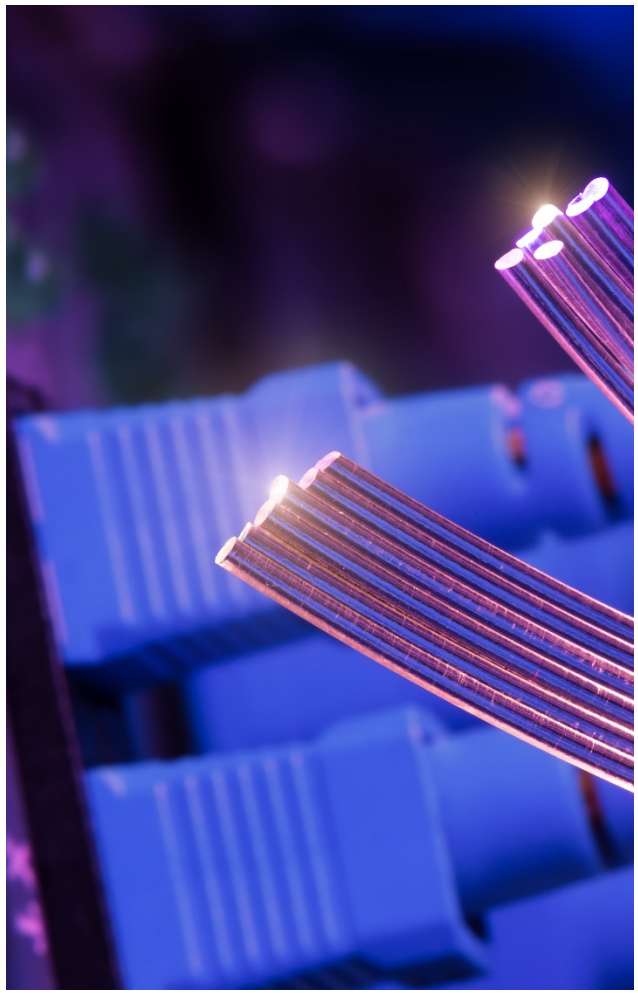
CLIFFORD
CHANCE

GDPR FOR INVESTMENT FUNDS

JOËLLE HAUSER
ISABELLE COMHAIRE

26 MARCH 2018

TABLE OF CONTENTS



1. GDPR HIGH LEVEL PRESENTATION

STATUS AND TIMING

- GDPR entered into force on 25 May 2016. It will become fully applicable after a 2 year transition period, i.e. on **25 May 2018**
  - **Regulation** rather than a directive: The GDPR will have a **direct effect** in all EU Member States
  - Greater harmonisation **BUT**: Member States can provide for **more specific rules in certain area** (e.g. employment context)
- Repealing of the law of 2 August 2002 on the protection of persons with regard to the processing of personal data (DPL)

WHAT IS DATA PROTECTION ABOUT?

A set of rules on the “processing” of “personal data” of “data subjects”

- **Processing**: any operation or set of operations which is performed on personal data whether or not by automated means
- **Personal data**: all information relating to an identified or identifiable natural person
  - Includes professional, trivial and/or public data
  - Includes data that allow identification indirectly (e.g. an online identifier such as an IP address can be personal data if it can be linked to the individual)
  - Legal entities are not protected BUT the individuals working for these entities/representatives of the companies are protected
  - “Sensitive” or “special categories” of personal data (health, racial or ethnic origin, religious/philosophical beliefs, political opinions, trade union membership)
- **Pseudonymized data**: remains personal data **however** it is viewed as a highly recommended risk-reduction technique

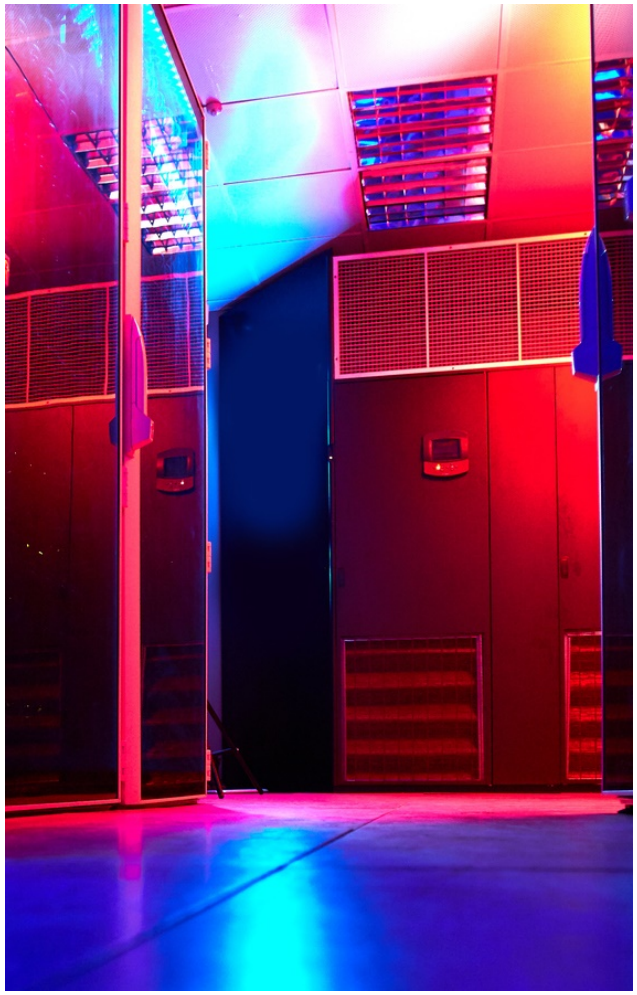
CONTROLLER/PROCESSOR

- **Data Controller**
  - Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
  - **Joint data controllers**: when there is more than one controller in respect of processing the same data for the same specific purpose
- **Data Processor**
  - Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- **A question of fact**
- **Obligations when having recourse to a data processor broadly unchanged BUT more extensive requirements for controller/processor contract**
  - Processing shall be governed by a **written contract or other legal act** which shall set out:
    - The subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller
    - In particular the Processor shall:
      - only **act upon instructions** of the controller (unless required to process data by Luxembourg or European Union law)
      - implement **appropriate organisational and security measures**
      - Assist the controller (to respond to data subject's request, in relation to data breaches, DPIA)
      - allow **audits**
      - when having recourse to a sub-processor, **imposes to the sub-processor the same obligations**
      - delete or return the personal data after the end of the services (unless EU or Luxembourg law requires storage of the personal data)
  - **Processor shall not enlist another processor** without the prior specific or general written consent of the controller
  - Controller liable UNLESS data processor
    - has violated its obligations as data processor
    - has acted outside the instructions of the data controller
    - has acted in contradiction to the licit instructions of the data controller

TERRITORIAL SCOPE OF THE GDPR

- Controllers and processors who have an establishment in the EU regardless of the geographic locations in which they process personal data
  - Offshoring does not avoid the GDPR

- Extra-territorial scope: Application of the GDPR to companies based outside of the EU if activities related to:
  - **offering of services or goods to individuals in the EU** (irrespective of whether a payment of the data subject is required)
  - **monitoring of the behaviour** of individuals in the EU

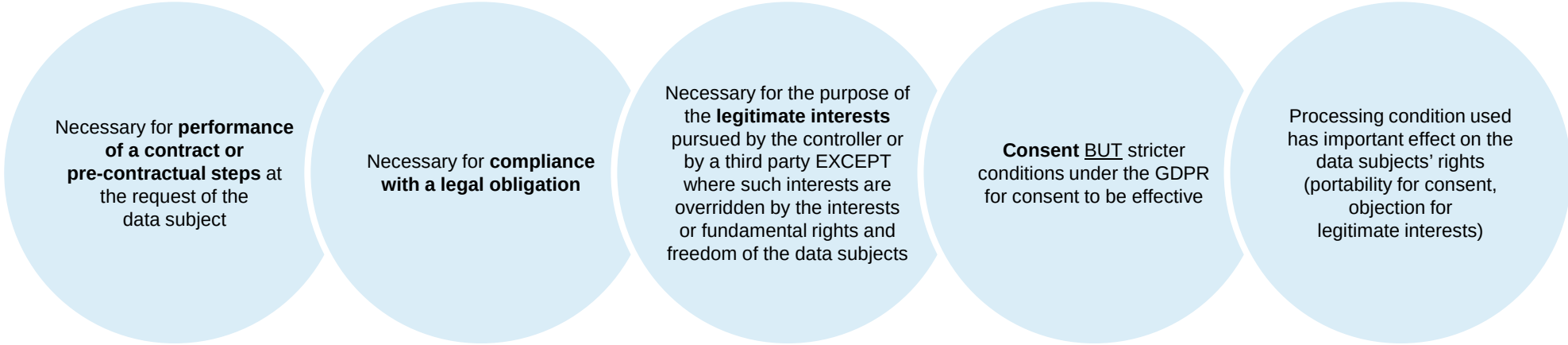


BASIC PRINCIPLES ARE (MOSTLY) NOT CHANGING

- **Lawfulness, fairness and transparency**
  - information must be provided **in writing**

    UNLESS data subject requests oral information
  - provided in concise, transparent, intelligible and easily accessible form
  - **Response** to be provided to data subject **within 1 month** of receipt of the request (2 additional months if the request is complex and shall be motivated)
  - **Free of charge** (or reasonable fee if request unfounded or excessive)
- **Proportionality**
  - **Purpose limitation**
  - **Data minimisation**
  - **Accuracy**
  - **Storage limitation**
- **Integrity and confidentiality**
- **Accountability**
  - Need to **demonstrate compliance**
  - Need to create and maintain **records of processing**
    - NOT applicable to companies employing fewer than 250 persons UNLESS the processing they carry out:
      - is likely to result in a risk to the rights and freedoms of data subjects,
      - is not occasional,
      - includes special categories of data or criminal convictions and offences data
- **Privacy by design/ privacy by default**
- **Data protection officers**
  - The appointment of a DPO is required:
    - If the processing is carried out by a public authority
    - If the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subject on a large scale
    - If the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences
    - + May be imposed by Member States (not foreseen in the draft Bill 7184).
  - Possibility to appoint a single DPO at group level
- **Data protection impact assessment ("DPIA")**
  - Controllers to carry out DPIA when the processing is "likely to result in a high risk to the rights and freedoms of natural persons"
- **Security breach notification:**
  - Classification of breach: "Confidentiality breach", "Integrity breach", "Availability breach"
  - Controller to report security breaches (except for breaches unlikely to give rise to any risk) to the data protection authority
  - Controllers to inform affected data subjects of security breaches likely to result in a "high risk" to their "rights and freedoms"
  - Processors to inform controllers "without undue delay" when they become aware of security breaches affecting personal data
  - Timing of report: **within 72 hours** of becoming aware of the security breach

JUSTIFICATION FOR THE PROCESSING



INTERNATIONAL DATA TRANSFERS

- No restriction on transfer within EEA
- Transfer on the basis of an **adequacy decision**:
  - White list of countries

- Transfers subject to **appropriate safeguards**:
  - EU model contracts, “binding corporate rules”, approved code of conduct, and approved certification mechanisms
- Transfers made on the basis of a **limited set of conditions** (e.g. explicit consent)

RIGHTS OF THE DATA SUBJECTS

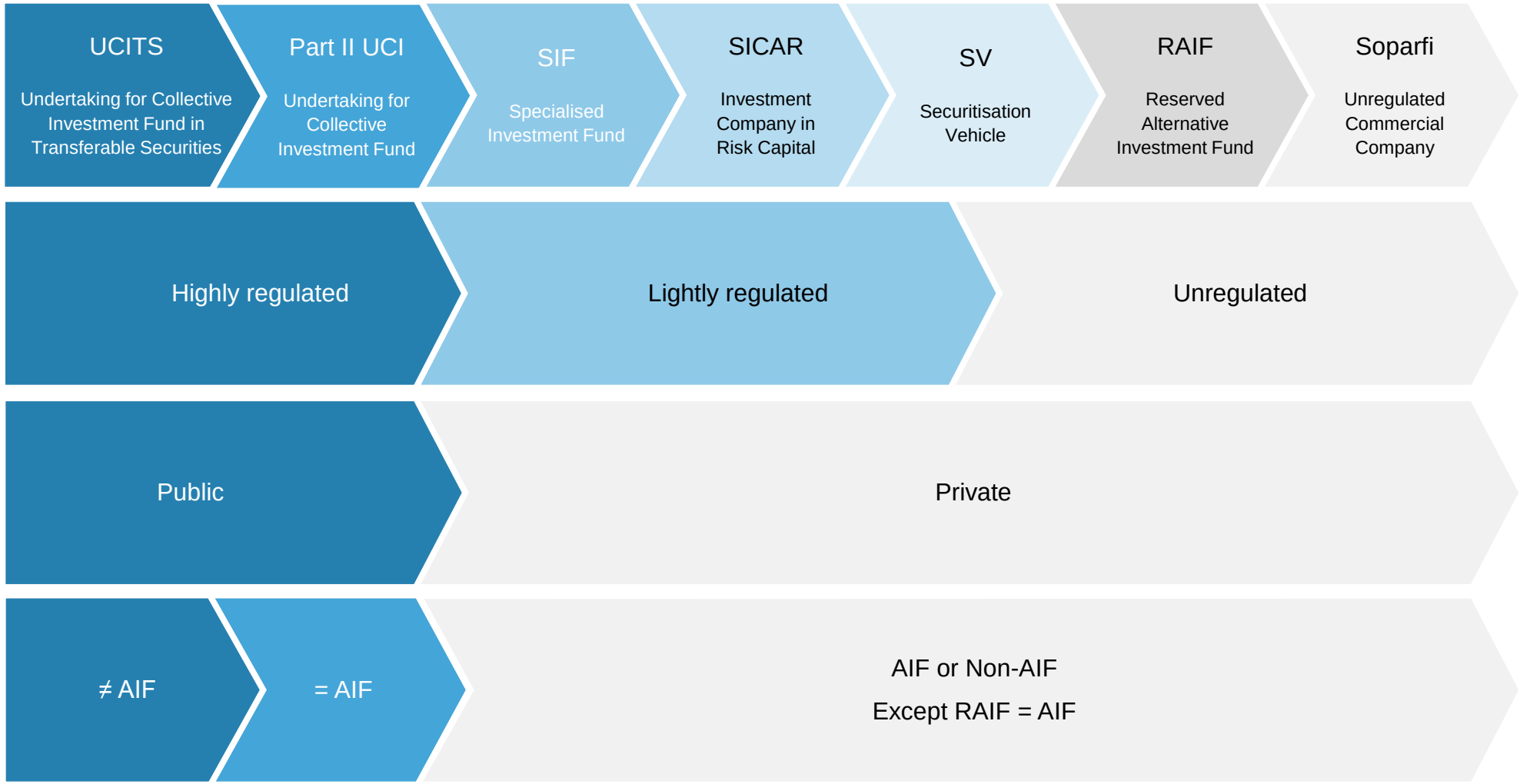
- Right to **information**
- Right of **access**
- Right to **rectification**
- Right to **object**
  - ! **Burden of proof reversed** – controller must demonstrate compelling legitimate grounds for processing
- Right **to be forgotten**
  - will not arise as long as the controller has a **legitimate reason** to continue processing the data
- Right to **data portability**
  - **Limited** to
    - data provided by the data subject
    - processing carried out by automated means, and
    - processing of data justified on the basis of consent or because it is necessary for the performance of a contract
  - **Does not apply**:
    - to data created by the company or obtained from third-party sources by the company
- Right to **restriction of processing**

SANCTIONS

- **Administrative fines** (new in Luxembourg)
  - up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (for “minor” infringement, e.g. absence of record of processing)
  - up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (e.g. data subjects’ rights, legitimacy of data processing, international data transfer provisions)
- **Regulatory actions** (not new but reinforced)
- **Civil sanctions** (not new but non-profit bodies can bring a representative action on behalf of individuals – class actions)
- **Criminal sanctions**?

2. GDPR IMPACT ON INVESTMENT FUNDS

LUXEMBOURG FUND STRUCTURING TOOLBOX



COMPARATIVE TABLE

	REGULATED INVESTMENT VEHICLES				UNREGULATED INVESTMENT VEHICLES	
	UCITS	**Part II UCI**	**SIF**	**SICAR**	**RAIF**	**Unregulated Company**
Applicable Legislation	Part I UCI Law	Part II UCI Law	SIF Law	SICAR Law	RAIF Law	Company Law
AIF Vehicle	No	Yes, unless exemption under AIFMD	Yes, unless exemption under AIFMD	Yes, unless exemption under AIFMD	Yes (no exemption as RAIF are always Full Scope AIFs)	Yes, if qualification as AIF and no benefit from any exemption
CSSF Supervision	Yes	Yes	Yes	Yes	No	No
Legal Forms	FCP SICAV (SA) SICAF (SA, SCA)	FCP SICAV (SA) SICAF (SA, SCA)	FCP SICAV/SICAF (SA, SCA, Sàrl, SCSA, SCS, SCSp)	~~FCP~~ SA, SCA, Sàrl, SCSA, SCS, SCSp (fixed or variable capital)	FCP (unless for RAIFs opting for special tax regime) SICAV/SICAF (SA, SCA, Sàrl, SCSA, SCS, SCSp)	~~FCP~~ SA, SCA, Sàrl, SCSA, SCS, SCSp (fixed capital only)
Multiple Sub-Funds Structure	Yes	Yes	Yes	Yes	Yes	No
Eligible Investors	Unrestricted	Unrestricted	Well-informed investors only	Well-informed investors only	Well-informed investors only	Unrestricted
ManCo Requirement	ManCo required for FCP and for SICAV/SICAF other than self-managed	ManCo required for FCP	ManCo required for FCP	No ManCo required	ManCo required for FCP	No ManCo required
AIFM Requirement	No	Yes if qualification as AIF and no benefit from any specific exemption • Full Scope AIF → Authorisation Regime: RAIFs as well as Part II UCIs, SIFs, SICARs and Unregulated Companies qualifying as so-called "Full Scope AIFs" (i.e. AIFs which cannot benefit from any of the exemptions under AIFMD), must designate a duly authorised and licensed AIFM, which can be an external AIFM or internal AIFM (i.e. internally-managed AIF) depending on their legal form (FCP/SICAV/SICAF/other AIF) ⇨ AIFMD Passport • Non-Full Scope AIF → AIFMD Registration Regime: For Part II UCIs SIFs, SICARs and Unregulated Companies that do not qualify as Full Scope AIFs (e.g. small AIFs, group AIFs, single investor AIFs, etc.), no authorised external/internal AIFM is required; but if they qualify as small AIFs under the de minimis exemption (i.e. AIFs below the €100/500 Mios thresholds under article 3(2) of the AIFMD) and do not chose to voluntarily opt in under the AIFMD to have an authorised AIFM, the simplified AIFM registration regime will apply to these entities that must appoint a registered AIFM (i.e. that is thus not authorised and licensed as AIFM by competent authorities), which can be external or internal AIFM depending on their legal form (FCP/SICAV/SICAF/other AIF) ⇨ No AIFMD Passport.				
Depositary Requirement	Yes	Yes	Yes	Yes	Yes	No unless Full Scope AIF
Other Required or Possible Service Providers	Central Administration, Investment Manager, Investment Adviser, Distributor, Auditor, Legal Adviser, etc. the case being in or outside EU					

INVESTMENT FUND DATA POTENTIAL PROCESSING

Generally, the purpose and business of investment funds is not to process personal data of natural persons

However, **investment funds**, as well as their managers and service providers, will be **directly involved in the processing of various personal data** that they receive, collect, store or use in their day-to-day activities with:

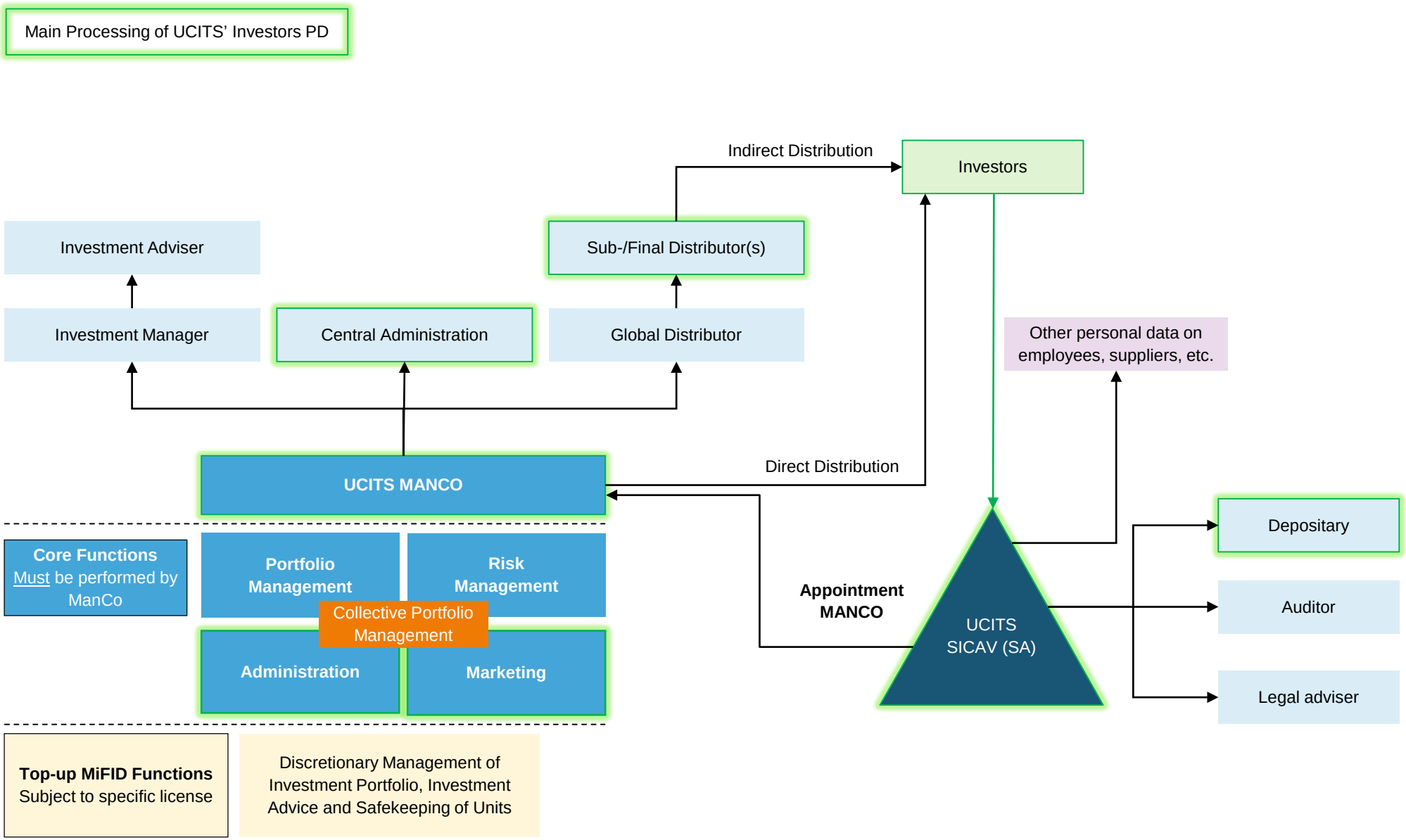
- **Investors/potential investors**, including retail investors and institutional, professional and other type of corporate/legal entity investors
  - Onboarding identification and investor suitability
  - AML/KYC
  - FATCA/CRS
  - Marketing
  - Other fund management and administration related processing (e.g. safekeeping of shareholder register, processing of subscription/redemption orders, payments of dividends/redemption proceeds, sending notices/reports to and otherwise notify/inform investors as per legal, regulatory or contractual requirements, complaint handling, etc.)
- **Own employees/staff members** (HR data)
- **Own directors/managers and other officers** which may but are not necessarily employees
- **Third party individual service providers/suppliers** or representatives of legal entity service providers/suppliers
- **Others**, such as EU individuals (e.g. online identifiers when visiting websites, etc.)

⇨ Sufficient for investment funds, and the case being their managers and service providers, to fall in scope of – and thus to have to comply with – GDPR, which does not distinguish between business sectors, the context of processing and/or the volume of processing

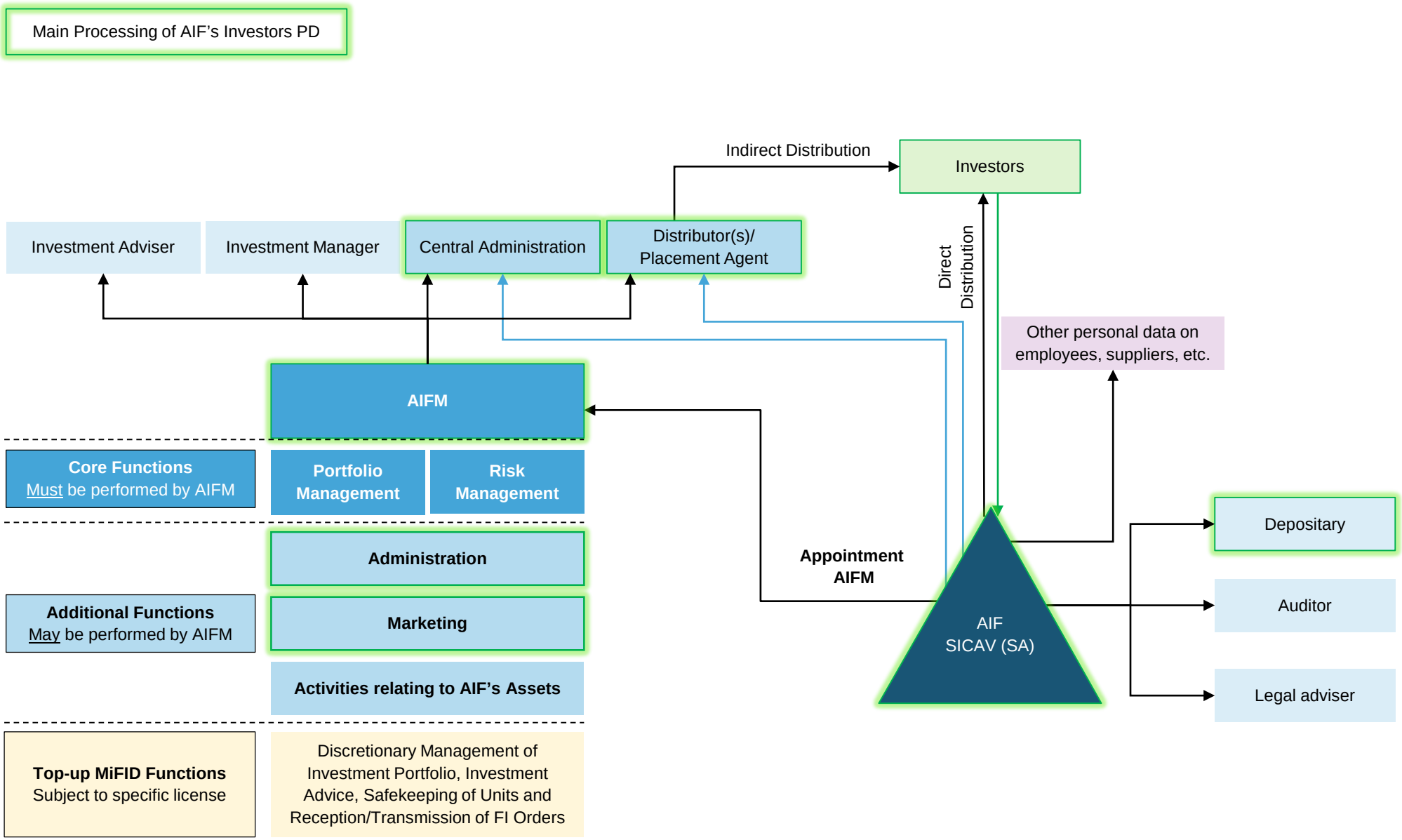
⇨ As minor an activity as consulting / collecting / storing / using / disclosing personal data constitutes “processing” sufficient to bring an organisation in the scope of GDPR

3. GDPR CASE STUDIES FOR UCITS AND AIF

ENVISAGED STRUCTURE OF UCITS



ENVISAGED STRUCTURE OF AIF



LIST OF RESPECTIVE OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS UNDER THE GDPR

Obligation	Data Controllers	Data Processors
Designate in writing a representative in the EU if not established in the EU	✓	✓
Implement appropriate technical and organizational measures	✓	✓
Procedure to respond to requests and complaints from data subjects	✓	
Notification of data breach	✓ (to authorities)	✓ (to data controllers)
Communication of data breach to data subjects	✓	
Records of data breach	✓	

LIST OF RESPECTIVE OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS UNDER THE GDPR (CONTINUED)

Obligation	Data Controllers	Data Processors
Cross-border data transfers justification (if applicable) (transfer permitted (i) to other countries ensuring "adequate" protection; (ii) on the basis of model contracts, binding corporate rules, approved code of conducts, approved certification mechanisms; (iii) with consent; (iv) to execute the contract; (v) if legitimate interests)	✓	✓
Written contract with processors / sub-processors (which shall stipulate in particular that Processor : (i) only act upon instructions of the controller (unless required to process data by Luxembourg or European Union law), (ii) implement appropriate organisational and security measures, (iii) allow audits, (iv) when having recourse to a sub-processor, imposes to the sub-processor the same obligations)	✓	✓
Prior written consent of the data controller to enlist another processor		✓
Arrangements for joint data controllers (to determine responsibilities)	✓	

LIST OF RESPECTIVE OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS UNDER THE GDPR (CONTINUED)

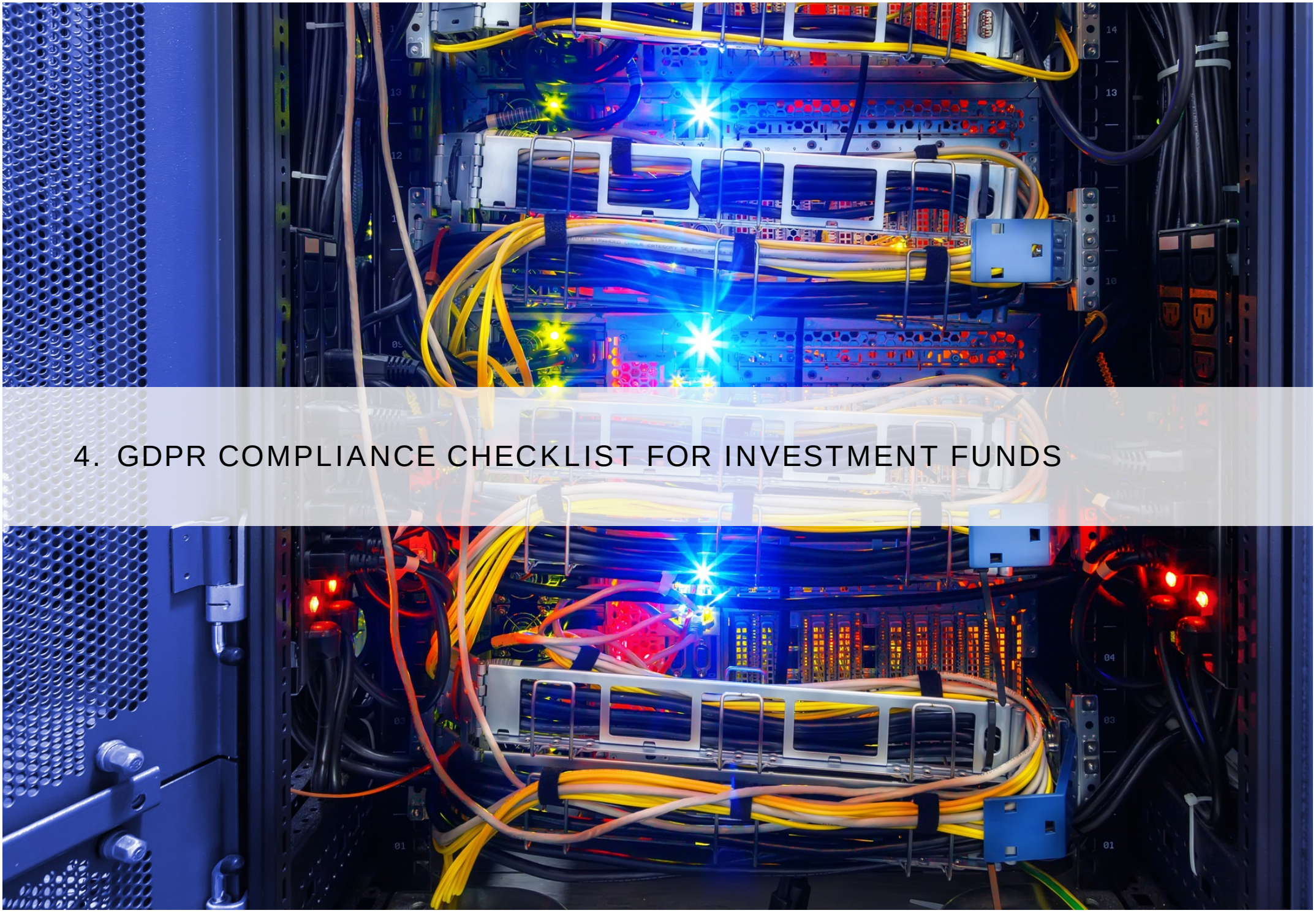
Obligation	Data Controllers	Data Processors
Designation of a DPO (if mandatory)	✓	✓
Records of processing activities	✓	✓ (processing carried out on behalf of a controller)
DPIA	✓	
Cooperation with authorities	✓	✓

IMPACT ON FUND DOCUMENTATION

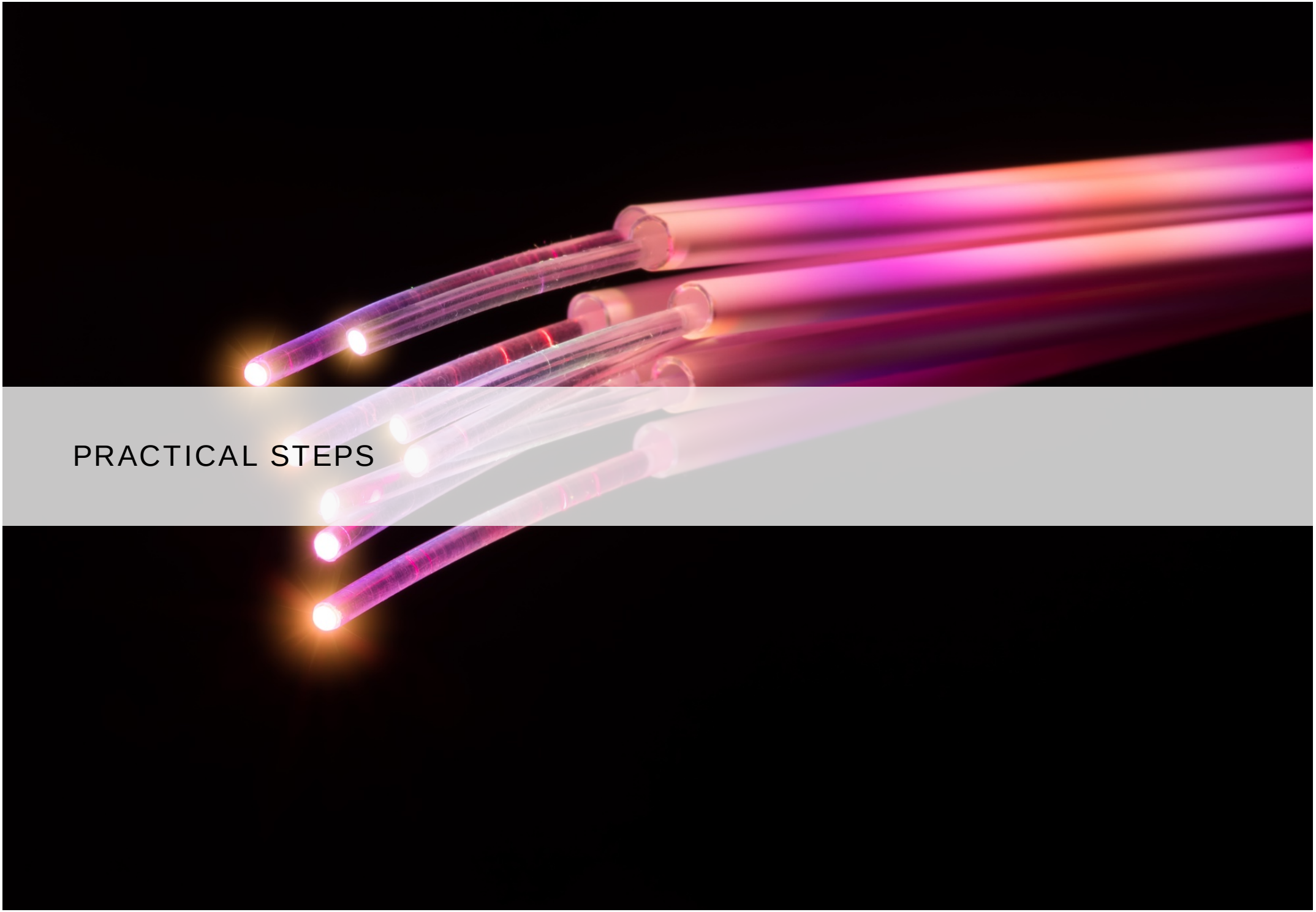
- **Information to the investors**
  - Responsibility of the data controller
    - Fund and/or ManCo (likely for the ManCo to contractually pass on to the Fund the obligation to inform the investors)
  - Information to be included:
    - in the PPM?
    - In the Subscription Form?
    - PPM sufficient if no reliance on consent, otherwise include in the Subscription agreement
    - if Information is sufficient (i.e. no consent required) full information on data processing does not compulsory need to be included in the PPM, BUT shall be provided elsewhere (website, registered office). A reference to the data protection notice in the PPM should be sufficient
- **Agreements**
  - consider whether service providers act as data processor and /or joint data controller
  - update all data controller – data processors 'agreements
    - include all information required under the GDPR
  - agreements to be reviewed: AIFM/ManCo Agreement, Central Administration Agreement, Depositary Agreement… [POMA]
  - ensure your contractors are informed about the processing of personal data that you are carrying out on their personal data (e.g. CRM,…)
- **Revised agreements should be submitted to the CSSF**

TRANSPARENCY

What information must be supplied?	Where data obtained directly from subject	Where data not obtained directly from subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data forms part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓



4. GDPR COMPLIANCE CHECKLIST FOR INVESTMENT FUNDS



PRACTICAL STEPS

IDENTIFICATION OF PERSONAL DATA PROCESSING
(TO START WITH)

- For non EU companies: Identify whether your organisation falls within the scope of the GDPR
- Need for a mapping of all personal data processing
- In relation to each personal data processing you have identified, ask yourself the following:
  - In **which capacity** do I process personal data: Am I a controller or a processor?
    - If controller, identify if there is a data processor
  - **What kind of personal data** is processed (employees, investors, third party service providers, etc..)?
    - Is sensitive data processed ?
    - What is the source of the data (individual itself?, processor?)
    - Is the data transferred to other group entities or third parties (and the location of these recipients)
  - **Why** personal data is processed (purposes)?
  - **On what legal basis** am I processing personal data (contract? consent? legal obligation? Legitimate interest?)
  - **Where** personal data is processed (location)?
  - **For how long** personal data is processed
  - **How** personal data is processed (security measures)

GAP ANALYSIS

- Ensure all personal data processing are compliant with the GDPR requirements
- Points of concern (not exhaustive):
  - Is the processing compliant with the core principles
    - E.g. is all personal data collected necessary for the purpose?
  - Is the legal basis used appropriate?
    - If relying on consent: Is the consent GDPR compliant?
  - Is the processing likely to result in a high risk to data subject?
    - Consider whether a data impact assessment is required

DOCUMENTATION AND PROCESSES
(! ACCOUNTABILITY PRINCIPLE)

- Put in place and/or update **data protection policies** (list not exhaustive)
  - Website privacy policy (including cookie policy)
  - Data protection policy
  - Impact assessment policy
  - Data breach policy
  - Record retention policy
  - **Ensure these policies are user friendly**

- Review and amend policies on **informing data subjects** and ensure you are ready to **respond to data subject's requests** (for information, rectification, access, portability, etc.)
  - Consider one-off communications to bring information that you have previously provided up to the GDPR standards
  - Consider if individuals are likely to exercise their new rights against you and what this means for your business in practice
  - Prepare a response package to address data subject objections
  - Build a case for all key processing operations which are not "optional" from the data subject's perspective
  - Be prepared to deal with objections swiftly
  - Consider circumstances in which the portability right may be used against you and, where portability would not be appropriate, how it can be avoided (for example, by relying on "legitimate interests" rather than "consent" to justify processing)
  - Where relevant, review systems and develop compliance plans to facilitate a low-cost response to portability requests

DOCUMENTATION AND PROCESSES
(! ACCOUNTABILITY PRINCIPLE) (CONTINUED)

- Keep **record of processing**
  - Record of processing shall be in writing, including in electronic form and should contain, depending on which capacity you act:

Controllers	Processors
Name and contact details of the controller and where appropriate, the joint controller, the controller's representative, and the data protection officer	Name and contact details of the processor and of each controller on behalf of which the processor is acting
Purpose of the processing	Categories of processing carried out on behalf of each controller
Description of the categories of data subjects	Transfers to a third country or international organisation, including the identification of that third country or organisation, and the safeguards put in place by the processor in the absence of an adequacy decision or other appropriate safeguards
Description of categories of personal data	Where possible, a general description of technical and organisational security measures used by the processor
Categories of recipients of personal data	
Transfers to a third country or international organisation, including the identification of that third country or organisation, and the safeguards put in place by the controller in the absence of an adequacy decision or other appropriate safeguards	
Where possible the envisaged time limits for the erasure of the different categories of the data	
Where possible, a general description of technical and organizational security measures used by the controller	

DOCUMENTATION AND PROCESSES
(! ACCOUNTABILITY PRINCIPLE) (CONTINUED)

- **International data transfers**
  - Map international data flows
  - Create international data transfer strategy
  - “Structural” solution for intra–group transfers?
- **Outsourcing management**
  - Identify key existing contracts which will extend beyond 25 May 2018
  - Renegotiate/update standard form processing agreements and contractual documentation
    - Consider the impact of the GDPR on warranties and indemnities (service providers may seek indemnity protection where following controller’s instructions)
    - Consider appropriate indemnity cover / risk allocation for sub–processor appointments
    - Consider cost impact for assessing whether controller instructions are GDPR compliant
- Analyse whether a **data protection officer** is required
  - Possibility to appoint a single DPO at group level
  - No official / informal position for Fund Industry in Luxembourg
- Consider whether a **data impact assessment** is required for new (and existing) technology
  - DPIA compulsory for processing operations initiated after 25 May 2018 BUT recommendation of the Article 29 Working Group to carry out DPIA for existing data processing
  - Examples of processing requiring a DPIA (Article 29 Working Group)
    - Monitoring of the employees’ use of the IT Tool
- Prepare for **data breach notifications**
  - Review security arrangements to ensure compliance
  - Build compliance into the contracting process for the engagement of new service providers (data processor to notify breaches “without undue delay”)
  - CNPD data breach notification form available online
- Integrate **privacy by design** and **default** into systems
  - Conduct a quantitative assessment on amount of personal data processed
  - Data minimisation:
    - Process data only necessary for a specific purpose
    - Delete data when no longer needed for the relevant purpose
    - Strong retention policy required
    - Favour technique such as: anonymisation, pseudonimisation, encryption
- Review security measures
  - Check security measures and incorporate appropriate safeguards to protect personal data

2 months left before the deadline

⇨ do not hesitate to contact us if you have any question

ISABELLE COMHAIRE

Counsel
T +352 48 50 50 1

E isabelle.comhaire@cliffordchance.com

CLIFFORD

CHANCE

Clifford Chance, 10 boulevard G.D. Charlotte, B.P. 1147, L-1011 Luxembourg, Grand-Duché de Luxembourg
© Clifford Chance 2018

WWW.CLIFFORDCHANCE.COM