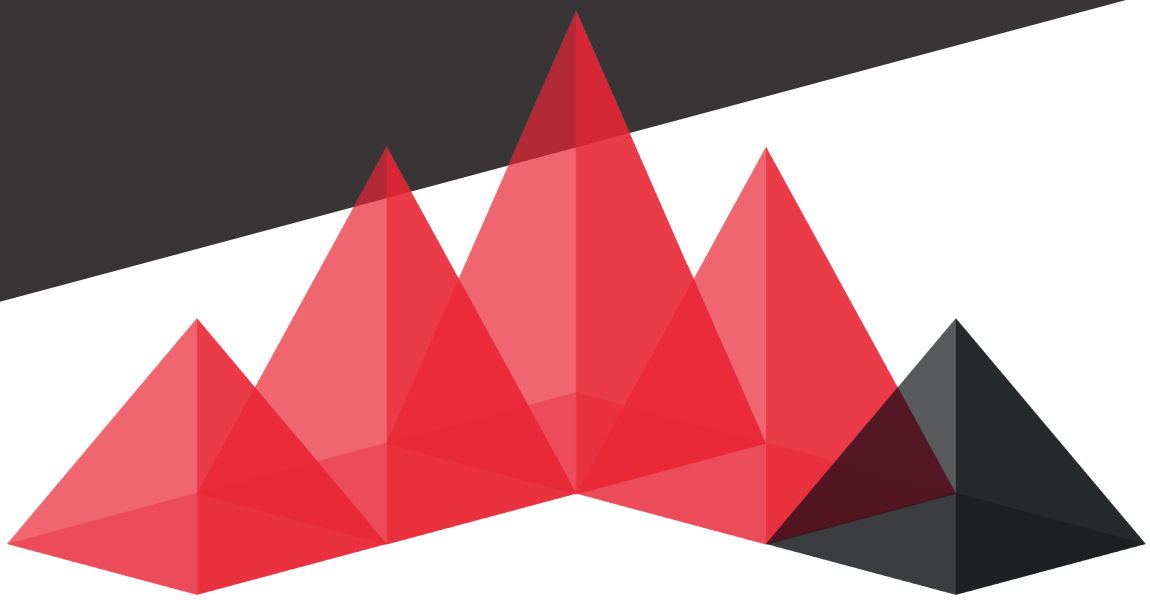
TALOS

Publikation



# Die neue Datenschutz - Grundverordnung (DSGVO)

**von Holger Barth**

---

## Anforderungen an die Umsetzung in den Fonds-Services am Standort Luxemburg

Aufgrund der jüngsten Entwicklungen der Digitalisierung, Globalisierung und des zunehmend komplexen Unternehmensumfeldes der EU, tritt erstmals ein einheitlicher Rechtsrahmen zum Schutz natürlicher Personen im Rahmen der Verarbeitung personenbezogener Daten in Kraft. Dieser geht zum 25. Mai 2018 unmittelbar in nationales Recht der EU-Mitgliedstaaten über.

Die tiefe Wertschöpfung sowie die spezifischen Geschäftsmodelle im Segment der Fonds-Services am Standort Luxemburg erhöhen die Komplexität der Umsetzungsanforderungen der DSGVO und bedürfen einer tiefergehenden Betrachtung.

TALOS

Publikation

**Was regelt die Datenschutz-Grundverordnung?**

Im Grundsatz regelt diese Verordnung den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, d.h. bei der:

- **Sammlung** *Erhebung, Erfassung*
- **Speicherung** *Erhebung, Erfassung*
- **Nutzung** *Anpassung, Verändern, Auslesen, Strukturierung, Abfrage, Verwendung, Verknüpfung, Abgleich*
- **Bereitstellung** *Offenlegung durch Übermittlung*
- **Vernichtung** *Einschränken, Löschen, Zerstörung*

aller Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen.

Damit werden durch die DSGVO, durch die die bisher gültige Datenschutzrichtlinie (95/46 EG) aus dem Jahre 1995 aufgehoben wird, die folgenden wesentlichen Anpassungen und Neuerungen für die sachlich und räumlich betroffenen Unternehmen relevant:

- **Rechenschaftspflichten**
  *Art. 5 Abs. 2.* Nachweis des Verantwortlichen, dass die Grundsätze für die Verarbeitung personenbezogener Daten (z.B. Zweckbindung, Datenminimierung, Richtigkeit) eingehalten werden

- **Informations- & Auskunftsrechte**
  *Art. 13 - 15.* Transparente, verständliche und leicht zugängliche Kundeninformationen sowie umfangreiche Auskunftsrechte gegenüber dem Datenverarbeiter

- **Datenschutzbeauftragten Organisation**
  *Art. 37 bis 39.* Ernennung eines Datenschutzbeauftragten sowie die Implementierung einer entsprechenden Aufbau- und Ablauforganisation

- **Meldepflicht**
  *Art. 33.* Meldung von Datenschutzverstößen innerhalb von 72 Stunden an die zuständige Datenschutzbehörde

- **Datenschutz-Folgenabschätzung**
  *Art. 35.* Auf einer Risikoanalyse basierende Abschätzung der Folgen vorgesehener Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch den Verantwortlichen

- **Einwilligung**
  *Art. 6.* Verarbeitung personenbezogener Daten bedarf der Einwilligung des Kunden

- **Privacy by Default**
  *Art. 25.* Sicherstellung der Einhaltung des Datenschutzes erfolgt bereits durch die datenschutzfreundliche Voreinstellung der für die Verarbeitung verwendeten technischen Mittel

- **Privacy by Design**
  *Art. 25.* Sicherstellung der Einhaltung des Datenschutzes erfolgt bereits durch das frühe Ergreifen technischer und organisatorischer Maßnahmen in der technologischen Entwicklung personenbezogener Verarbeitungsvorgänge

- **Datenübertragbarkeit**
  *Art. 20.* Recht der betroffenen Person, personenbezogene Daten anzufordern und auf einen anderen Verantwortlichen zu übertragen

- **Recht auf Vergessenwerden**
  *Art. 17.* Recht der betroffenen Person, sie betreffende Daten löschen zu lassen

- **Sanktionen**
  *Art. 83.* Geldbußen von bis zu 20 Mio. EUR oder 4% des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres

TALOS

Publikation

**Die Herausforderungen der DSGVO im Bereich der Fonds-Services**

## Die Herausforderungen

Die Umsetzung der DSGVO bringt die Unternehmen aller Branchen, die personenbezogene Daten verarbeiten, aufgrund der zahlreichen Anpassungen und Neuerungen vor dem zeitlichen aber auch vor dem erhöhten Sanktions- und Haftungsrisiko unter Handlungsdruck.

Aus unserer Sicht stellt das Verzeichnis der Verarbeitungstätigkeiten, in dem vollständig und strukturiert die Verarbeitung, Offenlegung und Löschung sowie die Beschreibung der verwendeten und implementierten technischen und organisatorischen Maßnahmen dokumentiert wird, die Basis dar. Dieses Verzeichnis ist zentral zur risikobasierten Implementierung geeigneter organisatorischer und technischer Maßnahmen, um sicherzustellen aber auch um nachzuweisen, dass die Verarbeitung in Übereinstimmung mit der Verordnung erfolgt.

Des Weiteren stellt die verpflichtende Installation einer Rolle des Datenschutzbeauftragten, sofern für die Verarbeitungsvorgänge umfangreiche regelmäßige und systematische Überwachungen von betroffenen Personen erforderlich sind, sowie die Zusammenarbeit mit den Aufsichtsbehörden die zentrale aufbauorganisatorische Herausforderung dar, sofern eine vergleichbare Organisation im Unternehmen nicht schon vorhanden war. Je nach Organisationsgrad des Unternehmens sowie der Komplexität des Geschäftsmodells und der eingesetzten Technologie wird sich der Zeit- und somit der Handlungsdruck für die Unternehmen erhöhen. Insbesondere auch dann, wenn es um die Umsetzung eines zentralen, grenzüberschreitenden Programmes mit der Konzernmutter geht in Kombination mit „off- oder near-shoring-Modellen“ in Bereich der Verarbeitungsprozesse.

## Die DSGVO im Bereich der Fonds-Services

Die Komplexität betreffend der Umsetzung der DSGVO im Bereich der Fonds-Services im Allgemeinen sowie am Standort Luxemburg im Besonderen ist zum einen dadurch determiniert, dass die Wertschöpfungskette in diesem Geschäftsfeld insgesamt sehr tief ist und zum anderen dadurch, dass viele Elemente der Wertschöpfung nicht in der eigenen Unternehmens-Gruppe erbracht werden, sondern auf spezialisierte Service-Provider externalisiert werden.

### Funktionale Betrachtung

Ausgangspunkt der Betrachtung der Umsetzungsverantwortung der DSGVO im Bereich der Fonds-Services ist die sog. regulatorisch verankerte Hauptverwaltungsfunktion, im Rahmen dessen:

- die Anlageverwaltung, d.h. das Portfolio- und das Risiko-Management,
- zusätzliche zentraladministrative Tätigkeiten, wie z.B. die Portfoliobewertung, die Fondspreisberechnung, die Abwicklung von Zeichnungen und Rücknahmen der Fondsanteile, und
- der Vertrieb des Fondsvehikels erfolgt.

In Abhängigkeit von den in Luxemburg existenten Fondsvehikeln UCITS[1] Teil I oder II des Gesetzes vom 17.12.2010, SIF[2] , RAIF[3] oder SICAR[4] und den gewählten juristischen Strukturen (FCP[5] , SICAV[6] , SICAF[7] ) übernimmt diese entweder die Verwaltungsgesellschaft oder eine selbstverwaltende Investmentgesellschaft (SICAV oder SICAF).

Kaum ein am Luxemburger Markt etabliertes Unternehmen nimmt alle Elemente der Hauptverwaltungsfunktion ganzheitlich in einer Unternehmensgruppe wahr. Vielmehr werden die einzelnen Elemente an Service-Provider delegiert, sei es im Sinne eines one-stop-shop-Modells an einen spezialisierten Service-Provider oder aber modular an unterschiedliche Anbieter.

1 Undertacking for Collective Investment in Transferrable Securities
2 Specialized Investment Fund
3 Reserved Alternative Investment Fund
4 Société d'Investissement en capital à risque
5 Fonds commun de placement
6 Société d'Investissement à Capital Variable
7 Société d'Investissement à Capital Fixe

TALOS

Publikation

## Die Herausforderungen der DSGVO im Bereich der Fonds-Services

Die Depotbankfunktion, auch wenn sie mit allen anderen Elementen der Fonds-Services durch einen Service-Provider gesamtheitlich übernommen wird, gehört nicht zur Hauptverwaltungsfunktion und kann somit nicht delegiert werden.

Unabhängig vom gewählten Modell und der Vielschichtigkeit der Provider-Struktur bleibt die Verantwortung der Hauptverwaltung bei der delegierenden Verwaltungsgesellschaft bzw. eigenver-walteten SICAV oder SICAF.

**Differenzierung data-controller und data-processor**

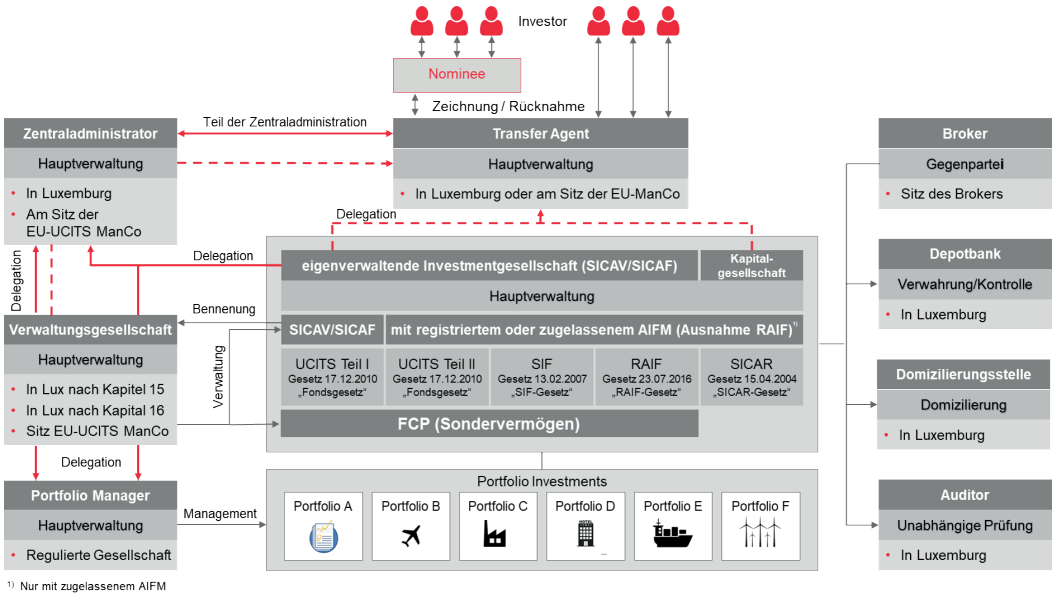
Ein wesentliches Element der DSGVO mit einem Impakt auf den Bereich der Fonds-Services ist die funktionale Differenzierung zwischen dem:

- Verantwortlichen (data-controller), der über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet, und dem
- Auftragsverarbeiter (data-processor), der die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet.

Die Tatsache, ob die Verarbeitung der personenbezogenen Daten operativ in der EU stattfindet, ist für die Anwendung der DSGVO nicht von Relevanz.

Durch den hohen Externalisierungsgrad von Elementen der Hauptverwaltungsfunktion in der luxemburgischen Fondsindustrie, wie das Portfolio-Management, die Fondsadministration und den Transfer Agent sowie die Vielzahl der fondsgeschäftsimmanent zu beauftragenden Service-Provider, wie die Depotbank sowie einen oder mehrere Broker, erfordern eine ganzheitliche Analyse und eine anschließende Umsetzung der Anforderungen aus der DSGVO.

Externalisierungen einzelner oder mehrerer Elemente der Hauptverwaltungsfunktion durch Delegation an spezialisierte Service-Provider (data-processor) mit dem Ziel der Reduktion der operativen Last und den damit verbundenen Kosten führen nicht dazu, dass der Board einer Verwaltungsgesellschfat oder einer selbstverwaltenden Investmentgesellschaft die Verantwortung über die Hauptverwaltung delegieren kann. Somit bleibt er de facto „data-controller“ auch wenn das operative Geschäftsmodell sich anders darstellt.




1) Nur mit zugelassenem AIFM

Abbildung 1:
Vehikel und Funktionen der Fonds-Services in LUX
(Quelle: Eigene Darstellung)

**Die praktische Umsetzung der DSGVO-Anfroderungen in den Fonds-Services**

## Vorgehensmodell zur praktischen Umsetzung der DSGVO Anforderungen in den Fonds-Services

Zur Umsetzung der DSGVO wendet TALOS ein erprobtes Transformationsmodell an. Zur Reduktion der Komplexität derartiger Transformationsvorhaben wird das spezifische Betriebsmodell einer die Hauptverwaltungsfunktion inne habenden Verwaltungsgesellschaft oder selbstverwaltenden Investmentgesellschaft in sechs Bausteine unterteilt und deren Abhängigkeiten untereinander identifiziert. Das Modell wird ergänzt durch den Transformationsprozess, der klare Ergebnisse für alle fünf Phasen festlegt.

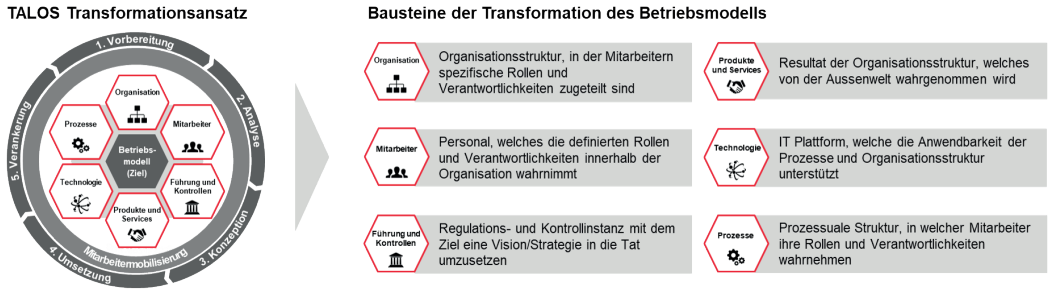



Abbildung 2:
TALOS Transformationsmodell
(Quelle: Eigene Darstellung)

## Sieben Kernbausteine zur Umsetzung der DSGVO Anforderungen in den Fonds-Services

In Anwendung dieses Modells und vor dem Hintergrund des bereits des stetig enger werdenden Umsetzungszeitfenster, sieht TALOS die folgenden umsetzungsrelevanten, wertschöpfungskettenübergreifenden Handlungsfelder bzw. Kernbausteine, um die Anforderungen aus der DSGVO im Bereich der Fonds-Services gerecht zu werden.

**Baustein 1:**
**Inventar der Verarbeitungstätigkeiten**
Analyse aller Applikationen und Geschäftsprozesse bezüglich Existenz, Kategorisierung und Schutzniveau personenbezogener Daten in der gesamten Wertschöpfung der Fonds-Services

**Baustein 2:**
**Sicherstellung der Datenschutzrechte**
Ist-Analyse der bestehender Datenschutzerklärungen und Kundeninformationen hinsichtlich eines potentiellen rechtlichen Anpassungsbedarfes. Analyse der Prozesse auf Basis des Inventars der Verarbeitungstätigkeiten hinsichtlich eines möglichen Anpassungs- und Entwicklungsbedarfes zur Beantwortung von Anfragen der Fondsinvestoren.

Sicherstellung, dass die Wahrung der Datenschutzrechte durch alle an der gesamten Wertschöpfung der Fonds-Services beteiligten Provider gewährleistet ist.

**Baustein 3:**
**Verträge mit Service-Providern**
Analyse bestehender Verträge im Rahmen der Delegation der Hauptverwaltungsfunktion hinsichtlich der Anforderungen zum Datenschutz.

**Baustein 4:**
**Rolle des Datenschutzbeauftragten**
Sicherstellung der richtlinienkonformen Installierung der Rolle eines Datenschutzbeauftragten (DSB) hinsichtlich Unabhängigkeit sowie Berichtswege in Innen- und Außenverhältnis gegenüber Board und den Aufsichtsbehörden.

**Die praktische Umsetzung der DSGVO-Anfroderungen in den Fonds-Services**

Definition klarer Zuständigkeiten und Verantwortlichkeiten der Rollen im Rahmen delegierter Elemente der Hauptverwaltungsfunktion. Abstimmung mit der Konzernmutter bei Gruppenlösungen. Identifikation, Dokumentation und Steuerung möglicher Interessenskonflikte, sofern dem DSB zusätzliche, über die gesetzlich verpflichtenden Aufgaben hinaus zugewiesen werden.

**Baustein 5:**
**Meldung Datenschutzverletzungen**
Sicherstellung, dass über die gesamte Wertschöpfung der Fonds-Services potentielle Schutzverletzungen identifiziert und gemeldet werden.

**Baustein 6:**
**Schulungsmaßnahmen**
Entwicklung und Durchführung eines Schulungsprogrammes für die Mitarbeiter zur Vermittlung der fachlichen Grundlagen und der Anforderungen aus der sowie der organisatorischen Änderungen durch die DSGVO. Sensibilisierung der Mitarbeiter hinsichtlich ihrer Rolle in der Wertschöpfung und der Verantwortung zum Schutz personenbezogener Daten im Rahmen deren Verarbeitung.

Entwicklung und Umsetzung eines Schulungskonzeptes für den DSB zur Vermittlung eines neuen Rollenverständnisses von der Umsetzung in die Überwachungsverantwortung.

**Baustein 7:**
**Ganzheitliche Koordination**
Sicherstellung einer holistischen Betrachtung der Umsetzung der Anforderungen aus der DSGVO. Synchronisierung der aufbau- und ablauforganisatorischen und datenverarbeitungstechnischen Veränderungsprozesse entlang der Wertschöpfungskette ausgehend von der Hauptverwaltung bis hin zu den delegierten Service-Providern.

Anpassung bestehender oder Entwicklung neuer Providermanagement- bzw. Provider-Auswahl- und Provider-Evaluationsprozesse vor dem Hintergrund der Einhaltung von Datenschutzverpflichtungen.

Analyse und die Integration des Risikos einer Datenschutzverletzung in die bestehenden Prozesse der Risikoidentifikation, -messung und –steuerung in Abhängigkeit des Setups des Betriebsmodells und der Delegationsintensität von Elementen der Hauptverwaltungsfunktion.

Definition einer Datenschutzstrategie, die gesamtheitlich mit allen Service-Providern in der Wertschöpfung verzahnt werden muss.

## Fazit

Die Anforderungen aus der DSGVO isoliert betrachtet sind vielfältig und setzten die Unternehmen durch die Sanktionsmechanismen, die bei einer Nichteinhaltung zu drastischen monetären aber auch zu reputativen Verlusten führen können. Durch die Tiefe der Wertschöpfungskette sowie Vielfalt der existierenden Betriebsmodelle am Finanzplatz Luxemburg mit unterschiedlichen einhergehenden Externalisierungsgraden, fehlt ein Standardmodell zur Umsetzung der DSGVO-Anforderungen. Vielmehr muss jede Gesellschaft betriebsmodellspezifisch die Auswirkungen analysieren und umsetzen. Eine konsequente Ausrichtung der Analysetätigkeiten an der gesetzlich kodifizierten Hauptverwaltungsfunktion für Verwaltungsgesellschaften und selbstverwaltende Investmentgesellschaften ist dabei fundamental.

TALOS

Publikation

**Wer wird sind**

TALOS definiert neue Standards in der Management Beratung. Als spezialisierte Boutique Beratung mit Schweizer Wurzeln und Büros in Zürich und Luxembourg beraten wir Kunden aus der Europäischen Finanzindustrie.

TALOS wurde 2008 von erfahrenen Management Beratern gegründet und ist seither zu einem etablierten Beratungsunternehmen für Finanzunternehmen gewachsen.

Als Experten für regulatorische und organisatorisch-operative Transformationslösungen decken wir die gesamte Bandbreite möglicher Fragestellungen ab, von der Analyse über die Strategie bis hin zur Umsetzung.

**Zürich**
TALOS Management Consultants
Bleicherweg 45
CH-8002 Zürich

**Luxembourg**
TALOS Management Consultants
5, Rue Heienhaff | 2nd floor (Wing E – Suite 2E)
L-1736, Senningerberg

www.talos-consultants.com

**Ihr Kontakt**

Holger ist Partner und Managing Director am Standort Luxemburg. Er verfügt über eine mehrjährige Erfahrung in der internationalen Finanzdienstleistungsindustrie. Er arbeitete in verschiedenen Führungsrollen für lokale und globale Kredit- und Finanzdienstleistungsinstitute, Fonds- und Versicherungsgesellschaften sowie Beratungsunternehmen mit dem Schwerpunkt im Bereich Asset Management, Asset Servicing, Fonds Administration, Transfer Agency, Fonds Brokerage sowie Depositary-, Private- und Retail Banking in Luxembourg und Deutschland. Holger stieß 2017 zu TALOS.

**Holger Barth**
Partner
Managing Director
+352 284878 2049
+352 671 886 091
holger.barth@talos-consultants.lu