MAINFIRST

DATEN-SCHUTZ-RICHTLINIE

MAINFIRST AFFILIATED FUND MANAGERS S.A.

10.2020

DATENSCHUTZRICHTLINIE

1. GELTUNGSBEREICH UND ZIEL

1.1 MainFirst Affiliated Fund Managers S.A. (die **Gesellschaft**) ist nach Artikel 101 Absatz (2) und Anhang II des Gesetzes von 2010 sowie nach Artikel 5 Absatz (2) und Anhang I des Gesetzes von 2013 zugelassen. Daneben ist die Gesellschaft zugelassen, folgende Dienstleistungen gemäß Artikel 5 Absatz (4) des Gesetzes von 2013 zu erbringen:

1.1.1 Verwaltung von Anlageportfolios, einschließlich solcher, die von Pensionsfonds und Einrichtungen der betrieblichen Altersversorgung gehalten werden, gemäß Artikel 19 Absatz (1) der Richtlinie 2003/41/EG und im Einklang mit von den Anlegern erteilten Einzelmandaten mit Ermessensspielraum; und

1.1.2 Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben.

1.2 Diese Richtlinie wird zur Einhaltung von Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (die Datenschutz-Grundverordnung „**DSGVO**“, und gemeinsam mit anderen einzelstaatlichen Gesetzen und Vorschriften das „**Datenschutzrecht**“) (die „**Richtlinie**“) bestimmt.

1.3 Die Richtlinie legt die Grundsätze für die Verarbeitung personenbezogener Daten fest, um sicherzustellen dass:

1.3.1 jede an der Verarbeitung personenbezogener Daten bei der Gesellschaft beteiligte Person die Anforderungen des Datenschutzrechts umfassend kennt und diese einhält; und

1.3.2 die betroffenen Personen über ihre Rechte gemäß Datenschutzrecht aufgeklärt werden.

2. DEFINITIONEN UND AUSLEGUNGEN

Definitionen

2.1 **Auftragsverarbeiter** hat die in Artikel 9.1genannte Bedeutung;

2.2 **Datenschutzrecht** hat die in Artikel 1.2genannte Bedeutung;

2.3 **Interner Datenschutzbeauftragter** ist die zum Datenschutzbeauftragten der Gesellschaft ernannte Person;

2.4 **Betroffene Person** bezeichnet die Person, deren personenbezogene Daten verarbeitet werden;

2.5 **EWR** bezeichnet den Europäischen Wirtschaftsraum;

2.6 **DGVO** hat die in Artikel 1.2genannte Bedeutung;

2.7 **Wesentliche Änderung** hat die in Artikel 18.3genannte Bedeutung;

2.8 **Wesentliche Verletzung** hat die in Artikel 17.2genannte Bedeutung;

2.9 **Personenbezogene Daten** bezeichnet Daten, die sich auf eine lebende Person beziehen, die anhand dieser Daten und anderer Informationen identifiziert werden kann, die sich im Besitz der Gesellschaft oder ihrer Vertreter oder Dienstleister befinden oder wahrscheinlich in deren

Besitz gelangen werden. Neben Sachinformationen zählen dazu auch Meinungsäußerungen über eine natürliche Person und jegliche Hinweise auf die Absichten der Gesellschaft oder einer anderen Person in Bezug auf eine natürliche Person.

2.10 Verarbeitung; und

2.11 **Sensible personenbezogene Daten** sind personenbezogene Daten in Bezug auf die rassische oder ethnische Herkunft der betroffenen Person, deren politische Meinungen, religiöse (oder weltanschauliche) Überzeugungen, ihren körperlichen oder geistigen Gesundheitszustand, Daten über Straftaten oder strafrechtliche Verurteilungen (unter anderem über begangene oder angeblich begangene Straftaten, Verfahren aufgrund von begangenen oder angeblich begangenen Straftaten und die Verfügung solcher Rechtsverfahren oder der Urteilsspruch eines Gerichts bei solchen Verfahren) sowie genetische und biometrische Daten.

Auslegungen

2.12 Sofern nichts anderes bestimmt wird, gilt für die vorliegende Richtlinie:

2.12.1 Überschriften werden nur zur einfacheren Bezugnahme eingefügt und wirken sich nicht auf die Auslegung aus;

2.12.2 die Begriffe „Artikel“ bzw. „Anhang“ bezeichnen einen Artikel oder Anhang dieser Richtlinie;

2.12.3 das Wort „oder“ wird nicht im engen Sinn verwendet;

2.12.4 der Begriff „Person“ beinhaltet auch Unternehmen, Körperschaften, Vereinigungen, Behörden oder Personengesellschaften;

2.12.5 „schriftlich“ bedeutet auch jede Art der Wiedergabe von Wörtern in lesbarer und dauerhafter Form;

2.12.6 Bezugnahmen auf ein Gesetz, eine Vorschrift oder Leitlinie bzw. eine Urkunde oder Teile derselben beinhalten jede Änderung, Modifizierung oder Neufassung davon; und

2.12.7 eine Bestätigung beinhaltet stets Verständnis und sofern erforderlich Zustimmung.

3. ALLGEMEINE GRUNDSÄTZE

Allgemeines

3.1 Alle Mitarbeiter, Berater und andere autorisierte Dritte, die Zugang zu personenbezogenen Daten haben, die von oder im Auftrag der Gesellschaft gehalten werden, müssen die Richtlinie einhalten.

Personenbezogene Daten

3.2 Die Gesellschaft verarbeitet nur personenbezogene Daten, die für ihren Kontakt zu einer bestimmten betroffenen Person unmittelbar relevant sind. Diese personenbezogenen Daten werden in Übereinstimmung mit dem Datenschutzrecht und der Richtlinie verarbeitet.

3.3 Bei sensiblen personenbezogenen Daten gelten strengere Regeln für die Verarbeitung.

3.4 Personenbezogene Daten werden allgemein von der Gesellschaft erhoben, um:

3.4.1 sicherzustellen, dass die Gesellschaft wirksame Geschäfte mit Dritten, einschließlich deren Kunden, Partnern, verbundenen oder angeschlossenen Unternehmen durchführen und ihre Pflichten und Rechte aufgrund von Verträgen mit diesen erfüllen bzw. ausüben kann;

3.4.2 ihre Mitarbeiter, Auftragnehmer, Beauftragten und Berater effizient zu verwalten;

3.4.3 ihr eine wirksame und effektive Geschäftsführung zu ermöglichen; und

3.4.4 alle gesetzlichen Verpflichtungen zu erfüllen.

3.5 Es werden die rechtmäßigen Gründe erläutert, aus denen personenbezogene Daten von der Gesellschaft verarbeitet werden können.

3.6 Personenbezogene Daten können innerhalb der Gesellschaft in Übereinstimmung mit den Datenschutzgrundsätzen und der Richtlinie offengelegt und von einer Abteilung an eine andere weitergegeben werden. Personenbezogene Daten werden auf keinen Fall an eine Abteilung oder Einzelperson innerhalb der Gesellschaft weitergegeben, die vernünftigerweise keinen Zugang zu den personenbezogenen Daten benötigt, um den Zweck zu erfüllen, für den diese erhoben wurden und verarbeitet werden.

3.7 Keine Abteilung oder Einzelperson innerhalb der Gesellschaft darf personenbezogene Daten aus einem anderen Grund verarbeiten, als für die rechtmäßigen Zwecke, für die sie erhoben wurden und verarbeitet werden.

4. DATENSCHUTZGRUNDSÄTZE

4.1 Jede Person, die personenbezogene Daten verarbeitet, muss folgende zentrale Grundsätze beachten:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

4.2 Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer nachvollziehbaren Weise verarbeitet werden. Niemand darf personenbezogene Daten verarbeiten, sofern er keinen rechtmäßigen Grund dazu hat und die betroffene Person darüber informiert hat, wie und weshalb er die betreffenden personenbezogenen Daten nach oder vor ihrer Erhebung verarbeiten wird.

Zweckbindung

4.3 Personenbezogene Daten dürfen nur für festgelegte und legitime Zwecke verarbeitet werden. Personenbezogene Daten dürfen nicht in einer Weise verarbeitet werden, die mit diesen Zwecken unvereinbar ist.

Datenminimierung

4.4 Die verarbeiteten personenbezogenen Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Richtigkeit

4.5 Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Personenbezogene Daten, die unrichtig sind, müssen unverzüglich berichtigt werden.

Datenspeicherung

4.6 Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, notwendig ist;

Rechte von betroffenen Personen

4.7 Personenbezogene Daten müssen im Einklang mit den Rechten der betroffenen Personen verarbeitet werden. Die betroffenen Personen haben das Recht, Kopien der sie betreffenden personenbezogenen Daten einzusehen, die Berichtigung unrichtiger Daten zu verlangen, Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen, die Zustimmung zur Verarbeitung zu widerrufen oder aus einem anderen wichtigen Grund die Löschung ihrer personenbezogenen Daten zu verlangen, wenn diese von der Gesellschaft nicht mehr benötigt werden.

Sicherheit

4.8 Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen gegen unbefugte oder unrechtmäßige Verarbeitung, unbeabsichtigten Verlust, unbeabsichtigte Zerstörung oder Beschädigung geschützt werden.

Internationale Datenübermittlung

4.9 Personenbezogene Daten dürfen nicht in ein Land oder Territorium außerhalb des EWR übertragen werden, sofern dieses Land oder Territorium nicht einen angemessenen Schutz der Rechte und Freiheiten der betroffenen Personen im Zusammenhang mit der Verarbeitung garantiert.

Rechenschaftspflicht

4.10 Die Gesellschaft und ihre externen Dienstleister sind für die Einhaltung dieser Richtlinie verantwortlich und müssen diese nachweisen.

5. EINWILLIGUNG

5.1 Personenbezogene Daten dürfen von der Gesellschaft nur verarbeitet werden, wenn der Zweck der Verarbeitung einem der gemäß Datenschutzrecht zulässigen Gründe entspricht. Personenbezogene Daten dürfen aus verschiedenen legitimen Gründen erhoben und verwendet werden. Unter anderem, wenn die betreffende Person eine Einwilligung zur Nutzung ihrer Daten abgegeben hat. Weitere geeignete Gründe sind in Artikel 8aufgeführt.

5.2 Wenn die Nutzung der personenbezogenen Daten einer Person auf der Grundlage einer Einwilligung erfolgt, muss diese alle nachfolgend aufgeführten Kriterien erfüllen:

5.2.1 die Einwilligung muss sich auf eine bestimmte Verarbeitung beschränken;

5.2.2 die betroffene Person muss ausführlich genug über die Verarbeitung informiert worden sein, um in der Lage sein, vollständig zu verstehen, wozu sie ihre Einwilligung erteilt;

5.2.3 die Einwilligung muss aus freiem Willen erteilt werden. Mit anderen Worten, die betroffene Person muss die Einwilligung aus freiem Willen erteilen. Eine Einwilligung wird nicht aus freiem Willen erteilt, wenn ein erhebliches Machtungleichgewicht besteht, demzufolge die betroffene Person keine freie Wahlmöglichkeit hat, ihre Einwilligung zu erteilen, beispielsweise in einem Beschäftigungskontext. Dennoch ist es unter Umständen möglich, eine gültige Einwilligung von einem Mitarbeiter einzuholen, wenn der Mitarbeiter die freie Wahl hat, seine Einwilligung zu erteilen (z. B. im Rahmen einer freiwilligen

Umfrage) oder der Mitarbeiter mit seiner Einwilligung einen gewissen Vorteil erzielt.

5.2.4 Die Erfüllung eines Vertrags oder die Erbringung einer Dienstleistung kann nicht an die Bedingung geknüpft werden, dass die betroffene Person ihre Einwilligung zur Datenverarbeitung erteilt, sofern die Datenverarbeitung nicht erforderlich ist, um den Vertrag zu erfüllen oder die Dienstleistung zu erbringen;

5.2.5 Die Einwilligung muss durch eine eindeutige Erklärung oder eine andere, klare, aktive Äußerung der betroffenen Person erfolgen, beispielsweise die Unterzeichnung eines Formulars. Die Einwilligung kann nicht stillschweigend oder passiv erteilt werden (z. B. durch zuvor angekreuzte Kästchen). Sofern die betroffene Person ein Mitarbeiter ist, muss die Einwilligung nach deutschem Recht schriftlich erfolgen, außer eine andere Form ist aufgrund besonderer Umstände angemessen; und

5.2.6 Die Einwilligung in die Verarbeitung personenbezogener Daten muss klar von anderen Zustimmungen abgegrenzt sein, die die betroffene Person erteilen soll (zum Beispiel darf sie nicht in die Bedingungen eines allgemeinen Vertrags eingebettet sein, den die betroffene Person unterzeichnen soll).

5.3 Wenn sich die Verarbeitung auf sensible personenbezogene Daten bezieht, muss die ausdrückliche Einwilligung der betroffenen Person eingeholt werden, im Idealfall durch eine unterzeichnete Erklärung oder auf sonstige Weise, aus der die Einwilligung der betroffenen Person eindeutig und nachweislich hervorgeht, oder auf eine andere Weise, aus der die Einwilligung der betroffenen Person ganz klar und nachweislich hervorgeht. Wie in Abschnitt 8 unten ausführlich beschrieben kann die Verarbeitung dieser sensiblen personenbezogenen Daten unter bestimmten Umständen ohne ausdrückliche Einwilligung erfolgen.

5.4 Die Gesellschaft sollte die Einwilligungen aufbewahren, um nachzuweisen, dass sie zur Verarbeitung der personenbezogenen Daten ermächtigt wurde.

5.5 Dabei ist zu beachten, dass eine betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Die betroffene Person sollte über dieses Recht informiert werden und der Widerruf der Einwilligung muss für die betroffene Person genauso leicht sein wie die ursprüngliche Erteilung. Es muss geeignete Verfahren geben, um die Einwilligung unverzüglich zu widerrufen.

6. VERARBEITUNGSZWECKE

6.1 In diesem Artikel werden die legitimen Gründe für die Verarbeitung genannt, die für die Verarbeitung durch die Gesellschaft höchstwahrscheinlich relevant sind. Wenn eine Verarbeitung nicht aus einem dieser Gründe erfolgt, sollte der interne Datenschutzbeauftragte kontaktiert werden oder, falls nach geltendem Recht kein interner Datenschutzbeauftragter erforderlich ist, sollte ein externer Datenschutzbeauftragte hinzugezogen werden, um Rat darüber einzuholen, ob die geplante Verarbeitung durchgeführt werden kann.

Nicht sensible personenbezogene Daten

6.2 Legitime Gründe für die Verarbeitung nicht sensibler personenbezogener Daten bestehen unter anderem:

6.2.1 wenn die betroffene Person ihre Einwilligung in die Verarbeitung erteilt hat;

6.2.2 wenn die Verarbeitung im legitimen Interesse der Gesellschaft erfolgt und keine ungebührenden Nachteile für die betroffene Person verursacht;

6.2.3 wenn die Verarbeitung für die Erfüllung eines Vertrages notwendig ist, an dem die betroffene Person als Partei beteiligt ist oder um (auf Verlangen der betroffenen Person) Schritte mit Blick auf den Abschluss einer Vereinbarung zu ergreifen; oder

6.2.4 sofern die Verarbeitung gesetzlich erforderlich ist.

Sensible personenbezogene Daten

6.3 Sensible personenbezogene Daten unterliegen strengeren gesetzlichen Kontrollen und die Umstände, unter denen sie verarbeitet werden können, sind stärker beschränkt als bei anderen personenbezogenen Daten. Zu den legitimen Gründen für die Verarbeitung sensibler personenbezogener Daten zählen unter anderem:

6.3.1 wenn die betroffene Person ausdrücklich ihre Einwilligung erteilt hat (dabei sind die oben genannten Anforderungen für die gültige Einwilligung und die möglichen Schwierigkeiten bei der Einholung einer gültigen Einwilligung in einem Beschäftigungskontext zu beachten);

6.3.2 wenn die Verarbeitung für die Erfüllung der Pflichte und Rechte der Gesellschaft oder der betroffenen Person aufgrund des Arbeitsrechts oder Sozialversicherungsrechts erforderlich ist;

6.3.3 für Zwecke des Arbeitsschutzes oder der Beurteilung der Arbeitsfähigkeit eines Mitarbeiters;

6.3.4 für Zwecke der Chancengleichheit, wenn die Verarbeitung erforderlich ist, um das Vorhandensein oder Nichtvorhandensein von Chancengleichheit oder Gleichbehandlung für bzw. von Personen unterschiedlicher Rasse oder unterschiedlichen ethnischen Ursprungs zu ermitteln oder zu überwachen, um diese Gleichheit zu fördern oder zu erhalten (obwohl es dafür keine Rechtsgrundlage in Luxemburg gibt); oder

6.3.5 wenn die Verarbeitung für gerichtliche Verfahren, die Einholung von Rechtsberatung oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

7. VERARBEITUNGSAKTIVITÄTEN MIT HOHEM RISIKO

7.1 Wenn die Verarbeitung von personenbezogenen Daten voraussichtlich ein hohes Risiko für die betroffene Person zur Folge hat (zum Beispiel, wenn sie eine besonders schwere Verletzung der Privatsphäre einer betroffenen Person darstellt), muss die Gesellschaft vor der Datenverarbeitung die potenziellen Auswirkungen der geplanten Verarbeitung auf die Rechte und Freiheiten der betroffenen Person bewerten. Die Bewertung der Auswirkungen wird von einem internen Datenschutzbeauftragten durchgeführt oder, wenn nach geltendem Recht kein interner Datenschutzbeauftragter erforderlich ist, vom externen Datenschutzbeauftragten.

7.2 Die Beobachtung oder das Profiling von betroffenen Personen, die Videoüberwachung von betroffenen Personen und die Verarbeitung sensibler personenbezogener Daten in großem Umfang stellen Verarbeitungsaktivitäten dar, die ein hohes Risiko darstellen.

8. VERARBEITUNG VON DATEN NACH TREU UND GLAUBEN

8.1 Alle Formulare (papier- oder webbasiert), auf denen Daten über eine natürliche Person erhoben werden, sollten eine Erklärung erhalten, in der dargelegt wird, wofür die Daten verwendet werden und wem sie offengelegt werden können.

8.2 Unabhängig davon, wie die personenbezogenen Daten erlangt werden (von der betroffenen Person oder von einem Dritten), müssen der betroffenen Person bestimmte Informationen über die Verarbeitung ihrer personenbezogenen Daten durch die Gesellschaft bereitgestellt werden. Diese Informationen müssen spätestens zum Zeitpunkt der Erhebung der personenbezogenen Daten bereitgestellt werden (oder wenn die personenbezogenen Daten von einem Dritten eingeholt werden, innerhalb einer angemessenen Frist nach Erhalt der personenbezogenen Daten oder bei der ersten Kommunikation mit der betroffenen Person, wobei der jeweils früheste Zeitpunkt maßgeblich ist.

8.3 Der betroffenen Person müssen unter anderem folgende Informationen bereitgestellt werden:

8.3.1 Identität und Kontaktdaten der Gesellschaft und des internen Datenschutzbeauftragten;

8.3.2 die Kategorien personenbezogener Daten, die in Bezug auf die betroffene Person erhoben werden;

8.3.3 wenn die personenbezogenen Daten nicht von der betroffenen Person eingeholt werden, die Quelle der personenbezogenen Daten;

8.3.4 der Zweck, zu dem die personenbezogenen Daten verarbeitet werden, einschließlich Rechtsgrundlage für die Verarbeitung. Wenn die Rechtsgrundlage berechtigte Interessen beinhaltet, muss auch eine Beschreibung der berechtigten Interessen mitgeliefert werden;

8.3.5 wenn personenbezogene Daten auf der Grundlage der Einwilligung der betroffenen Person verarbeitet werden, eine Erläuterung des Rechts der betroffenen Person, ihre Einwilligung jederzeit zu widerrufen;

8.3.6 die Kategorien personenbezogener Daten, die gegenüber Dritten offengelegt werden dürfen und die Gründe für diese Offenlegungen;

8.3.7 wenn eine vertragliche Verpflichtung zur Verarbeitung besteht, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten auf dieser Grundlage bereitzustellen, und mögliche Folgen, wenn die Informationen nicht bereitgestellt werden;

8.3.8 jede Absicht, die personenbezogenen Daten außerhalb des EWR zu übermitteln und Information über den Schutz, der für die übertragenen Daten dort besteht (mit ausführlichen Informationen darüber, wie die rechtlichen Anforderungen für die Übertragung erfüllt werden);

8.3.9 Informationen über das Bestehen automatischer Entscheidungsprozesse (zum Beispiel Profiling) der Gesellschaft auf der Grundlage personenbezogener Daten, unter anderem mit ausführlichen Informationen über die zugrunde liegende Logik und die Auswirkung auf die betroffene Person;

8.3.10 Dauer der Speicherung der personenbezogenen Daten oder (wenn die Angabe einer bestimmten Dauer nicht möglich ist), Kriterien, die für die Bestimmung der Speicherdauer verwendet werden;

8.3.11 generelle Beschreibung der Grundsätze und Praktiken der Gesellschaft in Bezug auf den Schutz der Vertraulichkeit und Sicherheit personenbezogener Daten;

8.3.12 Bestehen der Rechte der betroffenen Person; und

8.3.13 alle anderen Informationen, die erforderlich sind, um zu garantieren, dass die Verarbeitung nach Treu und Glauben erfolgt.

8.4 Diese Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitgestellt werden, sodass sie für die betroffene Person leicht verständlich sind.

8.5 Wenn sich die oben genannten Informationen, nachdem sie der betroffenen Person bereitgestellt wurden, ändern, muss der betroffenen Person ein aktualisiertes Exemplar der Informationen bereitgestellt werden.

9. EXTERNE DIENSTLEISTER

9.1 Wenn die Gesellschaft einen Dritten mit der Verarbeitung personenbezogener Daten im Auftrag der Gesellschaft beauftragt (ein **Auftragsverarbeiter**), muss der Auftragsverarbeiter eine schriftliche Vereinbarung mit der Gesellschaft abschließen, die:

9.1.1 ausführliche Angaben zu der Verarbeitung enthält, mit deren Durchführung dieser beauftragt wurde;

9.1.2 den Auftragsverarbeiter dazu verpflichtet, die personenbezogenen Daten ausschließlich gemäß den schriftlichen Anweisungen der Gesellschaft zu verarbeiten und sofern dies für ihn erforderlich ist, um seine Pflichten gegenüber der Gesellschaft gemäß der Vereinbarung zu erfüllen;

9.1.3 den Auftragsverarbeiter dazu verpflichtet, geeignete technische und organisatorische Maßnahmen und Kontrollen zu ergreifen, um die Vertraulichkeit und Sicherheit der personenbezogenen Daten sicherzustellen; und

9.1.4 jegliche zusätzlichen, gesetzlich vorgeschriebenen Pflichten im Zusammenhang mit der Verarbeitung festlegt. Eine Beratung über die zusätzlichen gesetzlich vorgeschriebenen Pflichten, die in der Vereinbarung enthalten sein müssen, ist beim internen Datenschutzbeauftragten erhältlich.

9.2 Die Vereinbarung sollte vom internen Datenschutzbeauftragten genehmigt und von beiden Parteien unterzeichnet werden, bevor jegliche personenbezogenen Daten an den Auftragsverarbeiter übermittelt werden.

9.3 Bei einem Vertragsabschluss mit einem Auftragsverarbeiter muss die Gesellschaft sowohl am Anfang der Beziehung als auch danach regelmäßig eine sorgfältige Prüfung durchführen, um sicherzustellen, dass der Auftragsverarbeiter in der Lage ist, die Anforderungen in Artikel 9.1einzuhalten und dass er diese auch tatsächlich einhält.

10. OFFENLEGUNG PERSONENBEZOGENER DATEN

10.1 Die Gesellschaft muss sicherstellen, dass personenbezogene Daten nicht an unbefugte Dritte offengelegt werden. Alle Mitarbeiter sollten vorsichtig sein, wenn sie aufgefordert werden, personenbezogene Daten an Dritte offenzulegen. Das gilt nicht für Auftragsverarbeiter.

10.2 Personenbezogene Daten sollten ohne Einwilligung der betroffenen Person und ohne Genehmigung des internen Datenschutzbeauftragten nicht schriftlich oder mündlich an Dritte weitergegeben werden.

10.3 In bestimmten Fällen ist die Offenlegung von personenbezogenen Daten ohne Einholung der vorherigen Einwilligung der betroffenen Person zulässig. Solche Offenlegungen können (abhängig von den Umständen) zulässig sein, wenn dies:

10.3.1 zum Schutz der nationalen Sicherheit erforderlich ist;

10.3.2 zur Verhinderung oder Aufdeckung von Straftaten, im wichtigen öffentlichen Interesse erforderlich ist und wenn die Einholung der Einwilligung von der betroffenen Person diesem Zweck schädlich wäre;

10.3.3 aufgrund der Rechtspflege erforderlich ist;

10.3.4 zur Einhaltung geltenden Rechts erforderlich ist; oder

10.3.5 zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich ist (wenn es um Leben und Tod geht), sofern deren Einwilligung nicht eingeholt werden kann.

10.4 Anträge auf personenbezogene Daten von Dritten müssen geeignete schriftliche Unterlagen beigefügt werden, und alle Offenlegungen müssen vom internen Datenschutzbeauftragten genehmigt werden.

11. ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

11.1 Die Übermittlung personenbezogener Daten außerhalb des EWR unterliegt speziellen rechtlichen Anforderungen. Die „Übermittlung" von Daten umfasst das Versenden von Daten in ein Drittland oder die Gestattung eines Fernzugriffs auf die Daten in einem Drittland, gleichgültig, ob die Gesellschaft die personenbezogenen Daten selbst außerhalb des EWR überträgt oder ein Auftragsverarbeiter dies im Auftrag der Gesellschaft tut.

11.2 Personenbezogene Daten dürfen nicht in ein Land außerhalb des EWR übertragen werden, sofern das Empfängerland nicht einen angemessenen Schutz der Rechte und Freiheiten der betroffenen Personen sicherstellt. Diese Anforderung kann erfüllt werden

11.2.1 durch Bestehen verbindlicher Unternehmensvorschriften (die nur für gruppeninterne Übertragungen relevant sind);

11.2.2 wenn für das Empfängerland eine „Angemessenheitsentscheidung" der Europäischen Kommission erfolgt ist (bislang ist nur für eine handvoll Länder wie die Schweiz, Kanada und Israel eine entsprechende Angemessenheitsentscheidung ergangen);

11.2.3 durch Abschluss einer Datenübertragungsvereinbarung mit der Gesellschaft und dem Drittland, das die personenbezogenen Daten enthält, die von der Europäischen Kommission genehmigte Standardvertragsklauseln enthält; oder

11.2.4 durch Zertifizierung eines US-Empfängers unter dem EU-US Privacy Shield.

11.3 Bevor eine solche Übertragung stattfindet, muss zunächst mit dem internen Datenschutzbeauftragten abgeklärt werden, ob die Übertragung rechtmäßig ist.

12. SPEICHERUNG UND VERNICHTUNG PERSONENBEZOGENEN DATEN

12.1 Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dazu muss für jede Kategorie personenbezogener Daten, die von der Gesellschaft verarbeitet werden, eine Speicherdauer festgelegt werden, die angesichts der gesetzlichen Gründe gerechtfertigt werden kann. Die Speicherdauer muss überwacht werden und nach Ablauf müssen die relevanten personenbezogenen Daten gelöscht oder anonymisiert werden (sodass eine Identifizierung der betroffenen Person, auf die sich die personenbezogenen Daten beziehen, nicht mehr möglich ist).

12.2 Zum Beispiel werden erhebliche Mengen personenbezogener Daten über Mitarbeiter erfasst. Sobald ein Mitarbeiter die Gesellschaft verlassen hat, brauchen nicht alle Daten von ihm gespeichert zu werden, weil viele davon, unter anderem die Bankverbindung für Gehaltszahlungen, lediglich zur Verwaltung des Beschäftigungsverhältnisses notwendig sind. Einige personenbezogene Daten müssen länger gespeichert werden als andere, beispielsweise wenn bestimmte Unterlagen aufbewahrt werden müssen, damit die Gesellschaft ihre gesetzlichen Pflichten einhalten kann.

12.3 Personenbezogene Daten müssen auf sichere Art vernichtet werden, sodass die Rechte und die Privatsphäre der betroffenen Personen geschützt sind und eine dauerhafte Löschung der personenbezogenen Daten sichergestellt ist (z. B. durch Schreddern, Entsorgung als vertrauliche Unterlagen oder sichere elektronische Löschung). Festplatten mit nicht mehr benötigten personenbezogenen Daten müssen vor der Entsorgung vollständig gelöscht werden.

13. DATENSCHUTZ UND DATENSICHERHEIT

13.1 Die Gesellschaft sorgt dafür, dass alle Mitarbeiter, Auftragnehmer, Beauftragten, Berater, Partner und anderen Parteien, die im Auftrag der Gesellschaft arbeiten, bei der Verarbeitung Folgendes beachten:

13.2 Elektronisch oder in Papierform gespeicherte personenbezogene Daten müssen stets sicher aufbewahrt werden. Die Mitarbeiter, Berater und autorisierten Dritten der Gesellschaft müssen sicherstellen, dass geeignete technische und organisatorische Maßnahmen umgesetzt wurden, um eine(n) unbefugte(n) oder zufällige(n) Zugang, Nutzung Offenlegung, Verlust oder Beschädigung bei der Verarbeitung der personenbezogenen Daten zu verhindern (unter anderem, wenn diese gespeichert oder übertragen werden). Die Maßnahmen zum Datenschutz sind in der Datenschutzrichtlinie des Unternehmens aufgeführt. Zu den technischen Maßnahmen zählen unter anderem Verschlüsselungstechniken zum Schutz von elektronisch gespeicherten personenbezogenen Daten. Zu den organisatorischen Maßnahmen zählt unter anderem die Aufbewahrung von Papieraufzeichnungen mit personenbezogenen Daten in abschließbaren Schränken.

13.3 Wenn personenbezogene Daten verloren gehen, beschädigt, preisgegeben, fehlgeleitet, gestohlen oder auf sonstige Weise in nicht zulässiger Weise verarbeitet werden, muss eine Verletzung des Schutzes personenbezogener Daten gemeldet werden. Jede Verletzung ist unverzüglich dem internen Datenschutzbeauftragten oder falls nach geltendem Recht kein interner Datenschutzbeauftragter erforderlich ist, dem externen Datenschutzbeauftragten zu melden. Diese stellen sicher, dass alle nach geltendem Recht erforderlichen weiteren Schritte oder Mitteilungen erfolgen.

13.4 Dabei ist sorgfältig darauf zu achten, dass geeignete Sicherheitsmaßnahmen für die Löschung oder Entsorgung personenbezogener Daten in Übereinstimmung mit Artikel 14umgesetzt wurden.

13.5 Personenbezogene Daten dürfen ausschließlich in Übereinstimmung mit Artikel 11 und 12offengelegt werden.

14. RECHTE DER BETROFFENEN PERSONEN

14.1 Betroffene Personen sind berechtigt, bestimmte Rechte in Bezug auf ihre personenbezogenen Daten auszuüben. Hierzu zählt das Recht auf Zugang zu den von der Gesellschaft über sie gespeicherten personenbezogenen Daten, das Recht auf Berichtigung ihrer Daten (wenn diese unrichtig sind) und unter bestimmten Umständen das Recht, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen oder ihre Löschung zu verlangen.

14.2 Betroffene Personen haben eine Reihe von gesetzlichen Rechten an ihren personenbezogenen Daten. Dazu zählen:

14.2.1 das Recht, Informationen über die Verarbeitung ihrer personenbezogenen Daten und Zugang zu den sie betreffenden, von der Gesellschaft gespeicherten (oder im Auftrag der Gesellschaft gespeicherten) personenbezogenen Daten zu erhalten;

14.2.2 das Recht, eine Kopie aller sie betreffenden von der Gesellschaft verarbeiteten personenbezogenen Daten zu erhalten, unter anderem (unter bestimmten Umständen) das Recht, die betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und das Recht zu verlangen, dass diese personenbezogenen Daten an einen Dritten übermittelt werden, sofern dies technisch machbar ist;

14.2.3 das Recht zu verlangen, dass die Gesellschaft die betreffenden personenbezogenen Daten berichtigt, wenn diese unrichtig oder unvollständig sind;

14.2.4 das Recht zu verlangen, dass die betreffenden personenbezogenen Daten unter bestimmten Umständen gelöscht werden. Das kann unter anderem unter folgenden Umständen der Fall sein:

(a) wenn die Speicherung der betreffenden personenbezogenen Daten von der Gesellschaft für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig ist; oder

(b) die Gesellschaft darf die personenbezogenen Daten der betroffenen Person nur mit deren Einwilligung verarbeiten (weil kein anderer rechtmäßiger Grund für die Verarbeitung der personenbezogenen Daten vorliegt) und die betroffene Person widerruft ihre Einwilligung; und

(c) wenn das Recht, auf eine Beschwerde bei der zuständigen Datenschutzbehörde besteht, wenn die betroffene Person der Ansicht ist, dass die Gesellschaft ihre Rechte verletzt hat.

14.2.5 Alle Anträge betroffener Personen, eines der oben aufgeführten Rechte auszuüben, sind zu beachten. Die Datenverantwortlichen sind gesetzlich verpflichtet, diese Anträge innerhalb von einem Monat nach Eingang zu beantworten. Alle tatsächlichen oder mutmaßlichen Anträge einer betroffenen Person auf Ausübung der oben genannten Rechte sind unverzüglich an den internen Datenschutzbeauftragten weiterzuleiten.

14.3 Die Anträge auf Ausübung dieser Rechte sind nach Eingang an den internen Datenschutzbeauftragten zu übermitteln.

15. AUFZEICHNUNGEN

15.1 Innerhalb der Organisation müssen korrekte und aktuelle Aufzeichnungen über die Verarbeitung durch die Gesellschaft aufbewahrt werden. Diese müssen Folgendes beinhalten:

15.1.1 ausführliche Angaben zum Datenverantwortlichen und zum internen Datenschutzbeauftragten;

15.1.2 den Zweck der Verarbeitung;

15.1.3 die Kategorien betroffener Personen und Kategorien personenbezogener Daten

15.1.4 die Kategorien von Empfängern personenbezogener Daten;

15.1.5 die Kategorien von Übermittlungen personenbezogener Daten in Länder außerhalb des EWR;

15.1.6 die geplanten Fristen für die Löschung personenbezogener Daten (falls möglich); und

15.1.7 eine allgemeine Beschreibung der von der Gesellschaft angenommenen technischen und organisatorischen Sicherheitsmaßnahmen.

16. ROLLEN UND ZUSTÄNDIGKEITEN

16.1 Der Verwaltungsrat jedes Unternehmens der Gesellschaft ist letztlich dafür verantwortlich sicherzustellen, dass die Gesellschaft ihre jeweiligen gesetzlichen Pflichten erfüllt.

16.2 Der interne Datenschutzbeauftragte ist dafür verantwortlich:

16.2.1 den Verwaltungsrat über die Zuständigkeiten, Risiken und Probleme im Zusammenhang mit dem Datenschutz zu informieren;

16.2.2 alle Datenschutzverfahren und zugehörigen Richtlinien zu überprüfen;

16.2.3 Datenschutzschulungen und -beratungen für Mitarbeiter zu organisieren;

16.2.4 alle Datenschutzanfragen von Mitarbeitern zu bearbeiten;

16.2.5 alle Anträge von Einzelpersonen auf Einsicht in die von der Gesellschaft gespeicherten entsprechenden Daten zu bearbeiten (Zugangsanträge natürlicher Personen); und

16.2.6 Verträge oder Vereinbarungen mit Auftragsverarbeitern zu prüfen und zu genehmigen.

17. ESKALATIONSVERFAHREN

17.1 Wenn eine potenzielle Verletzung dieser Richtlinie festgestellt wird, muss der interne Datenschutzbeauftragte informiert werden.

17.2 Nach Eingang einer Meldung über eine potenzielle Verletzung beurteilt der interne Datenschutzbeauftragte, ob es sich um eine wesentliche Verletzung handelt (eine **wesentliche Verletzung**).

17.3 Wenn es sich bei der Verletzung um eine wesentliche Verletzung handelt, informiert der interne Datenschutzbeauftragte den Manager, der entscheidet, welche angemessenen Maßnahmen zu ergreifen sind.

17.4 Wenn es sich bei der Verletzung nicht um eine wesentliche Verletzung handelt, kann der interne Datenschutzbeauftragte die Maßnahmen ergreifen, die er für angemessen hält.

17.5 Der interne Datenschutzbeauftragte führt Aufzeichnungen über alle tatsächlichen und potenziellen Verletzungen gegen diese Richtlinie, die gemeldet wurden.

18. ÜBERWACHUNG, ÄNDERUNGEN UND CHRONIK DER ÄNDERUNGEN

18.1 Die Qualität und Angemessenheit der Durchführungsvereinbarungen und dieser Richtlinie werden von der Gesellschaft und vom internen Datenschutzbeauftragten durch Ex-ante- und Ex-post-Beurteilungen überwacht.

Ex-post-Beurteilungen

18.2 Die Gesellschaft überprüft daneben regelmäßig, ob diese Richtlinie wirksam ist, d. h. ob die Prozesse korrekt angewendet werden.

18.3 Bei dieser Prüfung gilt ein bedeutendes Ereignis, das sich auf die Rechtmäßigkeit der Verarbeitung gemäß dieser Richtlinie auswirken könnte, als **wesentliche Veränderung**. Wenn eine wesentliche Veränderung eingetreten ist, erwägt die Gesellschaft, diese Richtlinie zu ändern.

18.4 Die Prüfung wird von der Gesellschaft und vom internen Datenschutzbeauftragten durchgeführt.

Überprüfung der Richtlinie

18.5 Diese Richtlinie wird jährlich überprüft und falls notwendig unter Berücksichtigung

18.5.1 der Ergebnisse der Überprüfung geändert; und

18.5.2 Ad-hoc, wenn die Ergebnisse der Überwachung eine wesentliche Veränderung darstellen.

18.6 Diese Richtlinie wurde wie folgt aktualisiert:

Art der Änderung oder Überprüfung	**01. Oktober 2020**
Initiierung	MainFirst Affiliated Fund Managers S.A. Anja Richter, Data Protection Officer
Jährliche Überprüfung	2021