Privacy beleid

Arcona Capital Fund Management B.V.

Versie:	Door:	Actie:	Materiële wijzigingen:	Aangenomen bestuur:
1.0	H. Visscher	Review	Ja	12 mei 2021
1.0	Charco & Dique	Review Q2 2022	Nee	Nvt
2.0	C&D	Review 2023	Ja	21 maart 2024

1. Doel

Arcona Capital Fund Management B.V. (hierna **ACFM** of de **Directie**) verwerkt in haar bedrijfsprocessen persoonsgegevens. Dit betreft onder nadere persoonsgegevens van participanten, UBO's, medewerkers, sollicitanten en leveranciers (hierna **Persoongegevens**).

ACFM vindt het belangrijk dat met Persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. De verwerking van Persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren om schade door misbruik aan participanten, UBO's, medewerkers, sollicitanten en leveranciers en ACFM zelf te voorkomen.

Met dit beleidsdocument wordt vastgelegd hoe ACFM invulling geeft aan de rechten en verplichtingen uit de Algemene Verordening Gegevensbescherming (2016/679/EG, hierna **AVG**) en aanverwante wet- en regelgeving betreffende de bescherming van Persoonsgegevens.

2. Reikwijdte en Governance

Dit beleid is van toepassing op iedere verwerking van Persoonsgegevens door ACFM.

De Directie is verantwoordelijk voor (de uitvoering van) het beleid. Het beleid wordt periodiek maar minimaal elke twee jaar of indien daar aanleiding toe is geëvalueerd en zo nodig herzien. De Compliance Officer (hierna **CO**) ziet erop toe dat wordt gehandeld in overeenstemming met het beleid en de wet- en regelgeving met betrekking tot dit onderwerp.

ACFM heeft geen privacy officer benoemd. Deze taken zijn belegd bij de CO. De CO informeert en adviseert over de verplichtingen voortvloeiend uit de AVG en ziet toe op de naleving van deze verordening en andere wet- en regelgeving betreffende de bescherming van persoonsgegevens. De CO heeft een adviserende rol bij het uitvoeren van privacy impact assessments (hierna **PIA's**).

De CO vervult ten minste de volgende taken:

- De Directie en medewerkers van ACFM informeren en adviseren over hun verplichtingen inzake de verplichtingen uit de AVG en andere wet- en regelgeving betreffende de bescherming van Persoonsgegevens;
- Toezien op naleving vaan de AVG, van andere wet- en regelgeving betreffende de bescherming van Persoonsgegevens en van het beleid met betrekking tot de bescherming van Persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de Verwerking betrokken personeel;
- Samenwerken met de Autoriteit Persoonsgegevens en andere toezichthouders; en
- Contactpersoon voor de Autoriteit Persoonsgegevens, in direct overleg met de Directie.

3. Definities

Betrokkene: ieder natuurlijke persoon van wie persoonsgegevens worden verwerkt.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de Betrokkene"). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een *identificator* zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Verwerken: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke: de natuurlijke of rechtspersoon, een overheidsinstantie, een dienst, of ander orgaan die alleen, of samen met anderen, het doel van en de middelen van verwerking van de persoonsgegevens vaststelt (in casu ACFM).

Register: het register van verwerking als bedoeld in artikel 30 van de AVG.

4. Beginselen van Verwerking van Persoonsgegevens

Bij de verwerking van Persoonsgegevens staan de volgende beginselen voorop:

Rechtmatigheid: Verwerking van Persoonsgegevens is rechtmatig (d.w.z. vindt uitsluitend plaats voor doeleinden die gebaseerd kunnen worden op één van de rechtsgrondslagen die in de AVG worden gegeven)[1].

Eerlijkheid en Transparantie: Verwerking van Persoonsgegevens is behoorlijk en transparant.

Doelbinding: Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en vervolgens niet op onverenigbare wijze verder verwerkt.

Dataminimalisatie: Persoonsgegevens zijn adequaat en ter zake dienend en blijven beperkt tot datgene wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Juistheid: Persoonsgegevens zijn juist en worden zo nodig gewist of gerectificeerd.

Opslagbeperking: Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de Persoonsgegevens worden bewaard noodzakelijk is.

Integriteit en vertrouwelijkheid: Persoonsgegevens worden door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt dat een passende beveiliging gewaarborgd is.

Verantwoordingsplicht: Persoonsgegevens worden verwerkt onder de verantwoordelijkheid van ACFM die ervoor zorgt en kan aantonen dat verwerking voldoet aan de bepalingen van de AVG.

4.1 Toepassing beginselen van Verwerking van Persoonsgegevens

De beginselen van Verwerking van Persoonsgegevens worden op de volgende manieren toegepast bij ACFM.

Rechtmatigheid: Uitsluitend die Persoonsgegevens worden door ACFM opgevraagd bij de Betrokkenen die wettelijk vereist zijn voor identificatie doeleinden en die ACFM als beheerder van beleggingsfondsen in staat stellen met de persoon in kwestie zakelijke transacties te kunnen doen.

Eerlijkheid en transparantie: Medewerkers melden Betrokkene(n) waarom Persoonsgegevens worden opgevraagd en ook wat de gevolgen zijn wanneer de Persoonsgegevens niet worden verstrekt door de Betrokkene(n). Het niet verstrekken van Persoonsgegevens kan er bijvoorbeeld toe leiden dat een betaling niet mag worden uitgekeerd, omdat de Betrokkene(n) of erven van Betrokkene(n) niet kunnen worden geïdentificeerd.

Doelbinding: Bij het opvragen van Persoonsgegevens wordt vermeld voor welk doel de Persoonsgegevens worden ingezet. De Persoonsgegevens worden enkel voor het omschreven doel verwerkt. De Persoonsgegevens worden veelal opgevraagd vanwege de wettelijke

[1] Zie artikel 5 en 6 van de AVG voor de rechtmatigheid en de te onderscheiden grondslagen (waaronder uitvoering contract,wettelijke verplichting of toestemming van de Betrokkene).

verplichtingen die voortvloeien uit de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna **Wwft**).

Dataminimalisatie: Medewerkers geven duidelijk aan welke specifieke Persoonsgegevens zij nodig hebben om te voldoen aan wettelijke vereisten. Daarnaast geven zij ook aan welke informatie achterwege kan worden gelaten. Medewerkers vragen enkel de Persoonsgegevens van Betrokkene(n) die de wet vereist, daarbij worden de principes van noodzakelijkheid, proportionaliteit en subsidiariteit toegepast. Het komt bijvoorbeeld veelal voor dat een Betrokkene is overleden en ACFM de erven moet identificeren alvorens tot uitkering over te gaan. In eerste instantie wordt er intern overlegd of de gegevens van de erven niet al zijn medegedeeld in eerdere correspondentie (subsidiariteit). Als dit niet het geval is of de gegevens niet compleet zijn, dan wordt vastgesteld welke informatie wettelijk vereist is alvorens de Betrokkene te benaderen (noodzakelijkheid en proportionaliteit).

Juistheid: Betrokkenen hebben zelf de verantwoordelijkheid ACFM te informeren omtrent veranderingen in hun Persoonsgegevens. Daarnaast zijn medewerkers ook actief bezig met het opvragen van Persoonsgegevens als deze onjuist blijken te zijn, bijvoorbeeld wanneer (nieuws)brieven retour worden gestuurd of e-mails niet worden ontvangen. Onjuiste Persoonsgegevens worden in een gedeeld bestand direct verwijderd en/ of aangepast naar de actuele gegevens.

Opslagbeperking: Verouderde Persoonsgegevens worden in het cliëntenbestand direct verwijderd en vervangen door de actuele persoonsgegevens als een betrokkene een wijziging doorgeeft. Daarbij worden enkel de nieuwe persoonsgegevens bewaard. Daarnaast worden paspoorten en identiteitsbewijzen direct verwijdert zodra de relevante gegevens zijn verwerkt.

Integriteit en vertrouwelijkheid: Persoonsgegevens worden technisch beveiligd door toegangscodes en zijn enkel toegankelijk voor medewerkers met een functie waarvoor de gegevens van belang zijn. Daarnaast worden fysieke gegevens veilig bewaard achter gesloten deuren. Onder 8. Beveiliging en andere beheersmaatregelen wordt verder ingegaan op de beveiliging van Persoonsgegevens bij ACFM.

Verantwoordingsplicht: Er worden meerdere maatregelen getroffen om te verzekeren dat er wordt voldaan aan de wettelijke vereisten vanuit de AVG bij het hele gegevensverwerkingsproces en alle daarbij betrokken partijen. ACFM legt verantwoording af aan de AFM Daarnaast heeft ACFM een externe Compliance Officer die samen met de CO monitort dat de verwerking van Persoonsgegevens voldoet aan de vereisten van de AVG.

5. Bijzondere categorieën van persoonsgegevens

Bijzondere categorieën van Persoonsgegevens zijn extra gevoelige gegevens zoals ras en etnische afkomst, politieke opvatting, religieuze overtuiging, vakbondslidmaatschap, gezondheid, seksuele geaardheid en strafrechtelijke veroordelingen.

In beginsel mogen bijzondere categorieën van Persoonsgegevens niet worden verwerkt, tenzij een specifieke uitzondering van toepassing is. Deze verschilt per categorie bijzondere Persoonsgegevens.

Persoonsgegevens van strafrechtelijke aard (waaronder een VOG) mogen worden verwerkt met de uitdrukkelijke toestemming van de Betrokkene.

Het Burgerservicenummer (hierna **BSN**) mag slechts worden gebruikt ter uitvoering van de betreffende wet of voor de doelen die bij wet zijn bepaald. ACFM vraagt geen BSN-nummers op van haar zakelijke relaties. Alleen ten behoeve van de verwerking van de salarisgegevens van het personeel en de commissarissen die in functie zijn van de door ACFM beheerde fondsen worden BSN nummers verwerkt. Tevens worden BSN-nummers verwerkt in de Insiderslist uit hoofde van de *Market Abuse Regulation*, hierna de **MAR**).

Vanaf september 2023 worden identiteitsbewijzen en paspoorten niet meer opgeslagen. De relevante gegevens voor het CDD-onderzoek worden opgeslagen in een overzicht, waarna de identiteitsbewijzen en paspoorten definitief worden verwijderd van de servers.

6. Register

De CO houdt een register bij waarin de verwerkingsactiviteiten staan waarvoor ACFM verantwoordelijk is. Het register bevat:

- Een beschrijving van de categorieën van Betrokkenen en van de categorieën van Persoonsgegevens;
- De verwerkingsdoeleinden;
- De categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- Indien van toepassing, doorgiften van Persoonsgegevens aan een derde land of een internationale organisatie. Daarbij worden ook de documenten inzake de passende waarborgen vermeld;
- De beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Als de verwerkingsactiviteit wijzigt, moet het Register daarop worden aangepast. De CO monitort de inhoud van dit Register.

In het Register worden niet de daadwerkelijke Persoonsgegevens van Betrokkenen opgeslagen. Het Register geeft slechts door middel van een beschrijving inzicht in de Verwerkingsactiviteiten. Het Register bevat dus een beschrijving van de Verwerkingsactiviteiten en niet de Persoonsgegevens zelf.

7. Rechten van Betrokkenen

Recht op informatie over de Verwerking

Indien de Persoonsgegevens van de Betrokkene worden verkregen, dient desgewenst informatie te worden gegeven over de volgende onderwerpen:

- De grondslag van de Verwerking;
- De verwerkers, en indien van toepassing het voornemen om de Persoonsgegevens te delen buiten Europa;
- De retentieperiode (of de bepaling daarvan) en over de overige rechten van de Betrokkene (zie hierna, alsmede vermelding van recht tot intrekking, klachtrecht); en
- De andere doeleinden van gebruik, indien van toepassing.

Voorgaande informatie hoeft niet te worden verstrekt, indien de Betrokkene al over deze informatie beschikt.

Indien de Persoonsgegevens niet van de Betrokkene zelf zijn verkregen, zal aan de Betrokkene aanvullend de volgende informatie worden verstrekt:

- De bron waar de gegevens vandaan komen en of deze bron openbaar is;
- Indien de Persoonsgegevens voor een ander doeleinde verwerkt worden zal aan de Betrokkene ook bovenstaande gegevens verstrekt moeten worden.

Ook hier geldt dat de informatie niet hoeft te worden gegeven als de Betrokkene al over de informatie beschikt, als het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen of als de Persoonsgegevens vertrouwelijk moeten blijven.

Recht van inzage: De Betrokkene heeft het recht van inzage in zijn/haar Persoonsgegevens.

Recht op beperking van de Verwerking: De Betrokkene heeft het recht om zijn/haar Persoonsgegevens in een Verwerking te laten beperken. Bij het ontvangen van een daartoe strekkend verzoek dient telkens te worden bepaald of dit kan worden uitgevoerd op rechtmatige gronden.

Recht van overdraagbaarheid (dataportabiliteit): De Betrokkene heeft het recht de hem/haar betreffende Persoonsgegevens, die hij aan Verwerkingsverantwoordelijke heeft verstrekt, in een gangbare vorm te verkrijgen en over te dragen. In een dergelijke situatie ontvangt de Betrokkene alle gegevens en draagt dit over aan een andere verwerkingsverantwoordelijke.

Recht van bezwaar: De Betrokkene heeft het recht om bezwaar te maken tegen de Verwerking van hem/haar betreffende Persoonsgegevens. Bij het ontvangen van een daartoe strekkend verzoek dient telkens te worden bepaald of dit kan worden uitgevoerd op rechtmatige gronden.

Recht van rectificatie en het wissen van gegevens: De Betrokkene heeft het recht om zijn/haar Persoonsgegevens te laten rectificeren of wissen. Bij het ontvangen van een daartoe strekkend verzoek dient telkens te worden bepaald of dit kan worden uitgevoerd op rechtmatige gronden.

De AVG kent een kennisgevingsplicht in geval van rectificatie of wissen van gegevens, en in geval van verwerkingsbeperkingen; iedere ontvanger aan wie Persoonsgegevens zijn verstrekt, moet in kennis worden gesteld van elke rectificatie, wissen van Persoonsgegevens of beperking van de Verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

7.1. Afhandelen van verzoeken van de Betrokkene

ACFM zal zo snel mogelijk gehoor geven aan de rechten van de Betrokkene en uiterlijk binnen vier weken na ontvangst van het verzoek informatie verstrekken over de wijze waarop aan het verzoek gehoor is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn, indien nodig, met nog eens twee maanden worden verlengd. Het voldoen aan het verzoek van de Betrokkene geschiedt kosteloos tenzij het verzoek ongegrond of buitensporig is. In dat laatste geval mag het verzoek ook om die reden worden afgewezen.

Indien wordt getwijfeld aan de identiteit van de natuurlijke persoon die het verzoek indient, mag aanvullende informatie worden opgevraagd ter bevestiging van de identiteit van de Betrokkene.

7.2. Klachten en schadevergoeding

De Betrokkene heeft het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens indien hij/zij van mening is dat bij de Verwerking van zijn/haar Persoonsgegevens de AVG niet is nageleefd.

De Betrokkene heeft mogelijk recht op een schadevergoeding voor geleden schade indien een inbreuk wordt gepleegd op zijn of haar Persoonsgegevens.

8. Beveiliging en andere beheersmaatregelen

Bij iedere Verwerking van Persoonsgegevens worden passende technische en organisatorische beheersmaatregelen zoals beschreven in het Register in acht genomen, rekening houdend met de risico's van de verwerking. De passende technische en organisatorische beheersmaatregelen worden periodiek geëvalueerd en daar waar nodig geactualiseerd. Tijdens het wekelijkse CDD-overleg wordt de verwerking en opslag van (nieuwe) Persoonsgegevens besproken. Met de IT-beheerder (I & O Netsys) wordt overlegd over bescherming van Persoonsgegevens op basis van behoefte.

Ter zake van iedere nieuwe Verwerking of voor iedere wijziging in de Verwerking van Persoonsgegevens wordt vooraf, tijdens en achteraf de kans (waarschijnlijkheid) en impact (ernst) van de risico's van de Verwerkingen voor de Persoonsgegevens bepaald. Voor risico's voor de rechten en vrijheden van Betrokkenen die als hoog ingeschat worden, worden privacy impact assessments (PIA's, ook wel gegevensbeschermingseffectbeoordelingen) uitgevoerd. Indien wordt besloten dat er geen maatregelen worden genomen om de risico's te mitigeren, moet de Autoriteit Persoonsgegevens voorafgaand aan de Verwerking geraadpleegd worden.

De beheersmaatregelen bestaan onder andere uit beveiliging van apparatuur, toegangsbeveiliging, informatiebeveiliging, awareness, mede strekkende tot voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van Persoonsgegevens en de apparatuur die voor de Verwerking wordt gebruikt. Op elke medewerker zijn laptop met Persoonsgegevens zit een toegangscode. Daarnaast zijn laptops beveiligd en mag alleen de IT-beheerder programma's downloaden of bewerken met toestemming van de contactpersoon bij ACFM.

Fysieke Persoonsgegevens bevinden zich in afgesloten kasten in een ruimte die elke dag wordt afgesloten door de medewerkers na werktijd. Er zijn drie medewerkers die de sleutel voor deze ruimte hebben. Deze ruimte bevindt zich in het kantoorpand na de voordeur en het alarm.

Er is een geheimhoudingsplicht ten aanzien van het beschermen van de Persoonsgegevens welke bekend is bij de werknemers van ACFM. Bij de ontwikkeling van nieuwe applicaties wordt rekening gehouden met de Betrokkenen en wordt er gekozen uit alternatieven die voor hen het minst bezwaarlijk zijn volgens de principes van 'privacy-by-design' en 'privacy-by-default'.

Medewerkers hebben toegang tot Persoonsgegevens op basis van het 'need-to-know' principe. Dit betekent dat medewerkers alleen toegang tot Persoonsgegevens hebben als zij deze nodig hebben om hun werkzaamheden te kunnen uitvoeren uit hoofde van hun functie. Compliance medewerkers hebben bijvoorbeeld toegang tot een Compliance map en specifieke gegevens voor hun werkzaamheden. Medewerkers van Asset Management daarentegen hebben geen toegang tot een Compliance map, maar juist andere bestanden en mappen afgestemd op hun werkzaamheden. Daarnaast heeft de IT-beheerder voor het toevoegen van mappen en bestanden op de computer van een medewerker de schriftelijke toestemming nodig van de contactpersoon bij ACFM, waardoor de directie zorgvuldig kan afstemmen welke medewerker tot welke map toegang heeft.

8.1. Dataretentie

De Persoonsgegevens mogen niet langer worden bewaard dan strikt noodzakelijk voor het doel waarvoor de gegevens zijn verzameld. In het overzicht dataretentie is per categorie

Persoonsgegevens vastgesteld na welke termijn deze moeten worden vernietigd. ACFM ziet erop toe dat met uitbestedingspartners of andere zakelijk relaties die inzage hebben in de Persoonsgegevens afspraken gemaakt worden over verwerking van Persoonsgegevens die vastgelegd worden in verwerkersovereenkomsten. Voor een aantal dienstverleners van ACFM zijn verwerkersovereenkomsten ondertekend.

9. Doorgeven van Persoonsgegevens aan derde landen

Persoonsgegevens worden opgeslagen op Sharepoint. Sharepoint betreft een platform van Microsoft. Microsoft heeft meerdere datacenters over de wereld, waaronder 14 binnen Europa. Persoonsgegevens worden in de meeste gevallen opgeslagen op de twee geografisch gezien dichtstbijzijnde datacenters om de impact van een natuurramp of uitval van de service te beperken. De dichtstbijzijnde datacenters bevinden zich in Nederland, Frankrijk of Duitsland.

De data van ACFM is daarom opgeslagen op servers binnen de Europese Unie (hierna **EU**), waardoor Microsoft verplicht is toepassing te geven aan het EU-US privacy shield framework.[2] Dit houdt in dat persoonsgegevens veilig kunnen worden gedeeld tussen de EU en bedrijven in de Verenigde Staten die zich houden aan het Data Privacy Framework.

Als er Persoonsgegevens worden doorgegeven aan landen buiten de EU ligt (derde land of internationale organisatie) moet aan vergelijkbare regels worden voldaan als bij de bescherming van Persoonsgegevens in Nederland/EU. ACFM zal uitsluitend Persoonsgegevens doorgeven in het geval van een adequaat beveiligingsniveau.

10. Meldplicht datalekken

In het geval dat Persoonsgegevens van Betrokkene(n) onbewust of onrechtmatig zijn gelekt (datalek), moet de Autoriteit Persoonsgegevens binnen 72 uur na het moment van constateren op de hoogte gebracht zijn, indien de inbreuk naar verwachting een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Daarnaast kan een plicht ontstaan om de Betrokkene op de hoogte te stellen van de inbreuk.

[2] https://blogs.microsoft.com/eupolicy/2022/03/25/eu-us-data-agreement-an-important-milestone-for-data-protection-microsoft-is-committed-to-doing-our-part/