Privacybeleid Stichting Pensioenfonds Croda

1. Algemeen

Binnen Stichting Pensioenfonds Croda (hierna: het fonds) wordt gewerkt met persoonsgegevens van actieve deelnemers, gewezen deelnemers, pensioengerechtigden en andere aanspraakgerechtigden (hierna: betrokkene of betrokkenen). Persoonsgegevens worden uitsluitend verwerkt voor het goed uitvoeren van de pensioenregeling en het nakomen van wettelijke verplichtingen. Betrokkene moet erop kunnen vertrouwen dat het fonds zorgvuldig en veilig met de persoonsgegevens omgaat.

Privacy speelt een belangrijke rol in de relatie tussen betrokkenen en het fonds en staat daarmee hoog op de bestuurlijke agenda. Het fonds is verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van betrokkenen. Het fonds geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van het fonds. Dit beleid bevat de minimale eisen voor de verwerking van persoonsgegevens en adequate en consistente voorzorgsmaatregelen voor het behandelen van persoonsgegevens door het fonds en door de verwerkers die door het fonds aangesteld zijn.

Dit beleid is van toepassing op de verwerking van persoonsgegevens van (onder andere) de (gewezen) deelnemers, pensioengerechtigden, andere aanspraakgerechtigden en van leveranciers van het fonds, via elektronische middelen of in systematisch toegankelijke papieren dossiersystemen en in archieven; ongeacht of die verwerking plaatsvindt door het fonds of door externe gegevensverwerkers namens het fonds. Bij de verwerking van persoonsgegevens dienen zij ook te voldoen aan de beleidsregels waarnaar in dit beleid verwezen wordt.

Het privacybeleid heeft raakvlakken met het risicomanagementbeleid en het uitbestedingsbeleid.

1.1 Definities

De volgende definities worden o.a. in de AVG gebruikt:

Autoriteit Persoonsgegevens: de nationale toezichthouder op de naleving van de Toepasselijke wet- en regelgeving;

Betrokkene(n): degene(n) op wie een Persoonsgegeven(s) betrekking heeft/hebben. De betrokkene is degene van wie de gegevens worden verwerkt;

Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

Derde(n): een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

Persoonsgegeven(s): 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;

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

Verwerkersovereenkomst: de overeenkomst die de verwerkingsverantwoordelijke sluit met de verwerker welke ten grondslag ligt aan de Verwerking van Persoonsgegevens, waarin alle afspraken rondom de verwerking zijn vastgelegd;

Verwerking van Persoonsgegeven(s): 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;

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

Profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

Toepasselijke wet- en regelgeving: de Algemene Verordening Gegevensbescherming (AVG) en/of de Nederlandse Uitvoeringswet AVG;

PIA: een Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling) dat wordt uitgevoerd indien een Verwerking van Persoonsgegevens een hoog risico oplevert voor de rechten en vrijheden van Betrokkene(n), gelet op de aard, omvang, context en doelen daarvan, een en ander conform de eventuele nadere concretisering door de Autoriteit Persoonsgegevens.

1.2 Doel

Het fonds koppelt privacybeleid aan thema's zoals governance, integriteit, kwaliteit en klantgerichtheid. De ambitie is het bereiken van een cultuur waarbinnen naleving van privacywetgeving vanzelfsprekend is.

Persoonsgegevens moeten altijd:

1. Rechtmatig worden verwerkt;
2. Beperkt tot het doel waarvoor zij zijn verkregen, worden verwerkt;
3. Ten aanzien van de betrokkene op transparante wijze worden verwerkt;
4. Toereikend en relevant zijn en beperkt tot het noodzakelijke in verband met de doelen waarvoor zij worden verwerkt;
5. Correct zijn en up-to-date (waar nodig bijgehouden worden);
6. Niet langer worden bewaard dan noodzakelijk in verband met de doelen waarvoor zij worden verwerkt en vervolgens worden vernietigd of geanonimiseerd;
7. Verwerkt worden met inachtneming van de rechten van de betrokkenen;
8. Passend beveiligd en vertrouwelijk behandeld worden;
9. Alleen worden verstrekt aan derden indien wettelijk toegestaan of vereist en op grond van een verwerkersovereenkomst en eventuele aanvullende vereiste bepalingen.

1.3 Gegevensverwerking

De hoofdregel van de verwerking van persoonsgegevens bij het fonds is, dat dit uitsluitend toegestaan is in overeenstemming met de in hoofdstuk 2.1 vastgelegde doeleinden en indien de verwerking op een zorgvuldige wijze plaatsvindt. Het fonds zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Voorkomen wordt dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft.

1.3.1 Soorten persoonsgegevens

Het fonds verwerkt de volgende soorten persoonsgegevens:

- Personalia, zoals naam, geboortedatum, geslacht, nationaliteit
- Contactgegevens, zoals adres(sen), e-mailadres(sen) en telefoonnummer(s)
- Burgerlijke staat, datum (einde) huwelijk, datum (einde) geregistreerd partnerschap, datum (einde) samenwonen
- Informatie over verwanten waaronder (gewezen) partner en kinderen, zoals personalia en contactgegevens
- Datum overlijden (gewezen) deelnemer, uitkeringsgerechtigde en verwanten
- Betalingsgegevens, zoals IBAN-rekeningnummer(s)
- Administratienummer
- Pensioenaanspraken en –rechten, pensioenverplichtingen
- Gegevens met het oog op het berekenen, vastleggen, en toedelen van pensioenaanspraken en –rechten en pensioenpremie, zoals loon- en dienstverbandgegevens
- Gegevens met het oog op het uitkeren van pensioenaanspraken, zoals identificatienummer (paspoort, rijbewijs, identiteitskaart)
- Gegevens betreffende klachten/geschillen
- Nummer sociale zekerheid (voor aangiftes bij de overheid), zoals in Nederland het Burger Service Nummer (BSN)
- Gegevens om de arbeidsongeschiktheid te kunnen vaststellen, o.a. gegevens van het UWV
- Andere gegevens die nodig zijn voor de uitvoering van (wettelijke) regelingen, zoals de Pensioenwet en sociale en fiscale wet- en regelgeving, waaronder loonaangifte Belastingdienst
- Gegevens over in- en uitgaande waardeoverdrachten
- Gegevens over vrijwillige voortzetting van de pensioendeelneming
- Toestemming voor het ontvangen van nieuwsbrieven
- Het IP-adres van de computer van betrokkene

Het fonds verwerkt geen bijzondere gegevens (met uitzondering van in beperkte mate gegevens over arbeidsongeschiktheid), zoals gegevens over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en het lidmaatschap van een vakvereniging of strafrechtelijke persoonsgegevens.

1.3.2 Categorieën betrokkenen

Het fonds verwerkt persoonsgegevens van de volgende categorieën betrokkenen:

a) (Gewezen) deelnemers / (ex-) werknemers
b) Pensioengerechtigden
c) (Ex-)partners van betrokkenen onder a. en b. (kinderen alleen bij overlijden)
d) Bezoekers website van het fonds
e) Functionarissen van het fonds (bestuursleden en leden van fondsorganen)
f) Contactpersonen van zakelijke relaties / dienstverleners van het fonds
g) Werkgevers

1.3.3 Verkrijging persoonsgegevens

Het fonds ontvangt persoonsgegevens ter verwerking van de volgende partijen:

a) Betrokkene of zijn wettelijke vertegenwoordiger;
b) (Oud-)werkgever van betrokkene of de van de door de (oud-)werkgever ingeschakelde salarisverwerker;
c) Basisregistratie Personen;
d) UWV;
e) Belastingdienst;
f) Stichting Pensioenregister;
g) Andere natuurlijke personen, instellingen en organisaties die door de betrokkene gemachtigd zijn tot het verstrekken van gegevens.

1.3.4 Ontvangers persoonsgegevens

Persoonsgegevens worden door het fonds verstrekt aan de volgende ontvangers:

a) Betrokkene of zijn wettelijke vertegenwoordiger;
b) (Oud-) werkgever van betrokkene of de van de door de (oud-) werkgever ingeschakelde salarisverwerker;
c) De belastingdienst;
d) (Her)verzekeraars;
e) Stichting Pensioenregister;
f) De pensioenuitvoerder die betrokken is bij een individuele of collectieve waardeoverdracht;
g) Andere natuurlijke personen, instellingen en organisaties die door betrokkene zijn gemachtigd om namens hen op te treden;
h) Overige derden voor zover dit noodzakelijk is voor de doelstelling, waaronder de door het fonds ingeschakelde gegevensverwerkers.

Het fonds informeert betrokkenen over het verwerken van persoonsgegevens. Het fonds heeft met de aangesloten werkgever schriftelijke afspraken gemaakt over het verstrekken van informatie bij indiensttreding van werknemers die gaan deelnemen aan de pensioenregeling van het fonds. Het fonds verstrekt aan de betrokkene – al dan niet via de aangesloten werkgever - de privacyverklaring van het fonds.

Als het fonds de persoonsgegevens wil gaan verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt het fonds betrokkenen vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

2. Wettelijk kader

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Pensioenwet, zijn de doelen voor het verwerken in de wet al vastgelegd. Daarnaast is het voor de uitvoering van de pensioenovereenkomst tussen de werknemer en de werkgever nodig dat persoonsgegevens verwerkt worden.

Het wettelijk kader wordt vanaf 25 mei 2018 in de basis gevormd door de Algemene Verordening Gegevensbescherming (AVG) ofwel General Data Protection Regulation (GDPR) en de Uitvoeringswet Algemene verordening gegevensbescherming. Door de vaststelling van dit privacybeleid geeft het bestuur van het fonds invulling aan haar wettelijke verantwoordelijkheid om te voorzien in privacybeleid volgens artikel 24 lid 2 van de AVG.

2.1 Doeleinden gegevensverwerking

Het fonds verzamelt en verwerkt de persoonsgegevens van betrokkenen ten behoeve van:

- het uitvoeren van de tussen de werkgever en de werknemer overeengekomen pensioenovereenkomst;
- het voldoen aan de wettelijke verplichtingen die op het fonds rusten (waaronder de Pensioenwet, de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG);
- het verstrekken van (wettelijke) communicatie aan betrokkenen;
- het functioneren van het fonds;
- het onderhouden van zakelijke relaties van het fonds;
- het waarborgen van de veiligheid en integriteit van het fonds daarbij ook inbegrepen het onderkennen, voorkomen, onderzoeken of bestrijden van strafbare of laakbare gedragingen gericht tegen het fonds en andere betrokkene(n).

2.2 Principes verwerking persoonsgegevens

De principes verwerking persoonsgegevens van het fonds ondersteunen het fonds en zijn verwerkers in hun streven aan de eisen van het privacybeleid te voldoen.

2.2.1 Rechtmatig verwerkt

Om persoonsgegevens op rechtmatige wijze te kunnen verwerken, moet aan bepaalde voorwaarden worden voldaan, zoals dat:

- de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waar de betrokkene partij bij is (bijvoorbeeld de pensioenovereenkomst, het pensioenreglement, de uitvoeringsovereenkomst);
- de verwerking voldoet aan de wettelijke verplichting waaraan het fonds gehouden is (bijvoorbeeld het melden van pensioengegevens van deelnemers en/of pensioenontvangers aan sociale zekerheids- of fiscale instanties);
- de betrokkene toestemming heeft verleend voor de verwerking (bijv. door een toestemmingsverklaring te ondertekenen voor het ontvangen van een nieuwsbrief, toestemming gebruik Cookies);
- de verwerking gerechtvaardigde belangen tot doel heeft die het fonds nastreeft (bijv. fysieke beveiliging, IT- en netwerkbeveiliging maar ook het bekleden van een functie voor het fonds dan wel werkzaam zijn voor het fonds);
- de verwerking noodzakelijk is om de vitale belangen van de betrokkene te beschermen (bijv. om beveiligings- of gezondheids- en veiligheidsredenen).

2.2.2 Verwerking voor beperkte doeleinden

Het fonds verwerkt persoonsgegevens uitsluitend voor de specifieke doelen of voor andere specifiek in de toepasselijke wet toegestane doelen. In de privacyverklaring van het fonds, zoals gepubliceerd op zijn website, staat uitgelegd op welke gronden, en voor welk doel de persoonsgegevens door het fonds worden verwerkt. Het fonds verwerkt persoonsgegevens uitsluitend om de pensioenregeling uit te kunnen voeren en te administreren. Ook verwerkt het persoonsgegevens voor naleving van wet- en regelgeving, waaronder identificatie, fiscale- en socialezekerheidswetgeving.

2.2.3 Transparante verwerking

Tenzij hiervoor een disproportionele inspanning nodig zou zijn, of tenzij de betrokkene zich hiervan aantoonbaar al bewust is, zal het fonds ervoor zorgen dat de betrokkene begrijpt wie de gegevensbeheerder is, voor welke doelen de gegevens verwerkt zullen worden, hoe de gegevens verwerkt zullen worden, wie degenen zijn aan wie de gegevens verstrekt kunnen worden, aan welke instantie de gegevens (eventueel) zullen worden overgedragen of hoe ze toegankelijk zullen zijn, en wat de rechten van betrokken zijn ten aanzien van hun gegevens volgens de geldende wet- en regelgeving. Deze informatie staat in de privacyverklaring van het fonds, zoals gepubliceerd op de website van het fonds. Die informatie wordt periodiek geëvalueerd en zo nodig aangepast.

2.2.4 Toereikend, relevant en beperkt tot het noodzakelijke

Persoonsgegevens worden door het fonds alleen verzameld en verder verwerkt voor zover dat noodzakelijk is voor de doelen van het fonds. Alle persoonsgegevens die niet nodig zijn voor deze doelen, worden niet verzameld. De verwerking van persoonsgegevens blijft beperkt tot gegevens die in redelijkheid geschikt en relevant zijn voor het desbetreffende doel. Er zijn maatregelen getroffen om persoonsgegevens niet langer te bewaren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.

2.2.5 Juiste verwerking

Persoonsgegevens moeten correct zijn en worden waar nodig bijgehouden. Er zijn maatregelen getroffen om de juistheid van persoonsgegevens te controleren, op het moment van verzamelen en met regelmatige tussenpozen erna en uiteraard ook als de persoonsgegevens tussentijds worden aangepast. Persoonsgegevens die onjuist of misleidend zijn, zijn niet correct; derhalve worden er in dat geval maatregelen getroffen om de juistheid van persoonsgegevens te controleren, op het moment van verzamelen en met regelmatige tussenpozen erna.

2.2.6 Niet langer bewaard dan noodzakelijk

Het fonds bewaart persoonsgegevens in haar administratie onder meer om vast te kunnen stellen of een pensioenaanspraak juist is vastgesteld of om vast te kunnen stellen of een claim op pensioen terecht is. Daarom behoeft het fonds het recht op “vergeten te worden” (gegevenswissing) niet te honoreren. De persoonsgegevens zijn gedurende een redelijke termijn na het bereiken van de pensioendatum nog nodig voor het doel waarvoor ze zijn verzameld of verwerkt. Het fonds werkt desgewenst mee aan het verwijderen van persoonsgegevens als dat moet op grond van een onrechtmatige verwerking of een wettelijke verplichting. Persoonsgegevens die het fonds niet bewaart worden veilig gewist. Niet-correcte of verouderde gegevens worden zo snel mogelijk vernietigd of gewist.

Dit artikel is anders voor verwerkers waarvoor de gegeven opdracht van beperkte duur is. Voor deze verwerkers is bepaald dat gegevens worden vernietigd op eerste aangeven van het fonds, dan wel conform contractuele afspraken die omtrent vernietiging zijn gemaakt.

2.2.7 Verwerkt met inachtneming rechten van betrokkenen

Persoonsgegevens worden op redelijke wijze en met inachtneming van de rechten van de betrokkene verwerkt. Het fonds heeft procedures geïmplementeerd om de volgende rechten van betrokkenen ten aanzien van hun persoonsgegevens te eerbiedigen, indien en voor zover de toepasselijke wet- en regelgeving hierin voorziet:

- Recht op inzage;
- Recht op rectificatie 1);
- Recht om "vergeten te worden" (gegevenswissing) 1);
- Recht op beperking van de verwerking 1);
- Recht op overdraagbaarheid (portabiliteit);
- Recht van bezwaar tegen de verwerking 1);
- Recht niet te worden onderworpen aan geautomatiseerde besluiten, waaronder profilering.

1) Deze rechten zullen (over het algemeen) alleen kunnen worden uitgeoefend door betrokkenen met betrekking tot de gegevens waarvoor betrokkene expliciet toestemming heeft gegeven voor de verwerking.

2.2.8 Veilig en vertrouwelijk behandeld

Het fonds neemt ter borging van integriteit en vertrouwelijkheid van persoonsgegevens passende technische en organisatorische maatregelen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Technische maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen (bijvoorbeeld toegangscontroles/autorisatie management, back ups, versleuteling van persoonsgegevens en beveiliging van transport van persoonsgegevens). Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van de persoonsgegevens (bijvoorbeeld het toekennen van verantwoordelijkheden en bevoegdheden, instructies en calamiteitplannen).

Indien wettelijke regels dit vereisen, zal het fonds de impact op de gegevensbescherming beoordelen van nieuwe initiatieven die vermoedelijk een hoog risico met zich meebrengen voor de privacy- en gegevensbeschermingsrechten van individuele personen en hiervan een registratie bijhouden.

2.2.9 Overdracht gegevens aan derden

Persoonsgegevens worden uitsluitend overgedragen aan derden (buiten het fonds) indien die overdracht voldoet aan de 'principes verwerking persoonsgegevens' en overige regels die zijn uiteengezet in dit privacybeleid en/of in toepasselijke privacy wet- en regelgeving. Een dergelijke overdracht zal uitsluitend plaatsvinden indien deze in het verlengde ligt van het doel waarvoor de gegevens verzameld zijn, en indien die overdracht voor dat doel noodzakelijk is.

Wanneer verwerking namens het fonds door een gegevensverwerker wordt verricht, wordt er door het fonds een schriftelijke overeenkomst (een verwerkingsovereenkomst) afgesloten of moet er een ander rechtsgeldig besluit zijn dat bindend is voor de gegevensverwerker. De gegevensverwerker dient de contractuele verplichtingen tot naleving van dit beleid en/of eventueel andere contractuele verplichtingen te accepteren voor zover die nodig zijn om een passend niveau van bescherming voor de overdracht en eventuele daarop volgende verwerking (inclusief latere overdrachten) te garanderen. De gegevensverwerker dient het fonds volledig te informeren ingeval er sprake is van een inbreuk op de beveiliging.

Soms kan het nodig zijn persoonsgegevens over te dragen aan andere derden die niet fungeren als gegevensverwerker voor het fonds, maar fungeren als verwerkingsverantwoordelijke. Een dergelijke overdracht is toegestaan, indien dit nodig is voor de uitvoering van een overeenkomst met de betrokkene (bijvoorbeeld herverzekeringen of accountantscontrole), indien de betrokkene zijn of haar toestemming heeft verleend, of om te voldoen aan dwingende bepalingen in nationaal recht, om juridische rechten te beschermen (bijvoorbeeld bij gerechtelijke procedures), of in noodsituaties waarin de overdracht noodzakelijk is om de vitale belangen van de betrokkene (bijvoorbeeld vanwege beveiligings- of gezondheids- en veiligheidsredenen) te beschermen.

2.3 Doorgifte van persoonsgegevens naar andere landen

Het fonds houdt zich aan wettelijke (ook Europese) verplichtingen die specifieke voorwaarden opleggen ten aanzien van internationale overdrachten van persoonsgegevens. Nederland heeft vooralsnog geen specifieke aanvullende voorwaarden ten aanzien van internationale overdrachten van persoonsgegevens. Het volgende is wel van toepassing: persoonsgegevens mogen uitsluitend worden overgedragen vanuit een land binnen de Europese Economische Ruimte (EER) naar landen buiten de EER ('externe landen') die door de Europese Commissie worden geacht over een passend beschermingsniveau te beschikken. De volledige en bijgewerkte lijst van besluiten inzake de doeltreffendheid van de bescherming van persoonsgegevens in externe landen door de Europese Commissie is in te zien op http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. Indien een extern land dit beschermingsniveau niet biedt, kunnen persoonsgegevens over het algemeen uitsluitend aan dit externe land worden overgedragen, indien het fonds en de gegevensimporteur standaard contractbepalingen aangaan die door de Europese Commissie zijn goedgekeurd.

3 Governance

3.1 Structuur

Het fonds verwerkt persoonsgegevens of laat deze door een verwerker verwerken in overeenstemming met de AVG. Om tot een adequate afdekking van de geïdentificeerde risico's te komen heeft het fonds de volgende taken en verantwoordelijkheden belegd bij de onderstaande functies:

Bestuur van het fonds
- Het bestuur van het fonds is eindverantwoordelijk voor het (laten) naleven van wetgeving en realiseert door goedkeuring van dit privacybeleid en de nadere uitwerking hiervan via procesbeschrijvingen het wettelijk vereiste niveau van bescherming van persoonsgegevens.
- Verantwoording afleggen over privacybeleidsvoering via het jaarverslag.

Eindverantwoordelijke Verwerker
- Stuurt op privacy-compliance.
- Draagt het privacybeleid van het fonds actief uit.

Medewerker Verwerker
- Gaat bewust om met de privacy van deelnemers, werkgevers, functionarissen van het fonds en collega's.
- Spant zich intensief in ter voorkoming van privacy incidenten.
- Meldt eventuele privacy incidenten direct conform de geldende procedure "melding datalekken".

Accountmanager/contactpersoon Verwerker
- Helpt privacyklachten tot een goed einde te brengen (ombudsfunctie).
- Adviseert de organisatie bij privacy-incidenten.
- Doet intern via (kwartaal)rapportages aan het bestuur verslag van de privacybeleidsvoering.

Internal audit
- Monitort toepassing, uitvoering en opvolging van beleid en richtlijnen ten aanzien van privacy en gegevensverwerking.

External audit
- Toetst het goed en betrouwbaar functioneren van de interne organisatie van het fonds. Het risico van privacy incidenten dient, zeker daar waar het gaat om privacy gevoelige processen, standaard te worden meegenomen in alle audits van systemen, processen en procedures.

3.2 Functionaris Gegevensbescherming (FG)

Het fonds heeft een FG aangesteld. Het fonds borgt op deze manier dat de verwerking van persoonsgegevens geschiedt volgens het opgestelde privacybeleid en compliant is met van toepassing zijnde wetgeving.

De werkzaamheden van de FG zijn:

- Het op peil houden van de benodigde kennis rondom de AVG en het fonds hierover gevraagd en ongevraagd informeren, adviseren en aanbevelingen doen; Toezicht houden op de AVG gerelateerde verwerkingen die worden gedaan door verwerkers en sub-verwerkers en overleg met die verwerkers;
- Optreden als contactpersoon richting de Autoriteit Persoonsgegevens;
- Melding doen van eventuele datalekken bij de Autoriteit Persoonsgegevens, binnen 72 uur;
- Het bijhouden van het register omtrent datalekken;
- Toezicht houden op plannen tot wijziging van systeemlandschap en processen, die dataprivacy gerelateerd zijn, van en door (sub-)verwerkers en indien nodig adviseren;
- Rapportage aan het fonds ingeval er calamiteiten zijn;
- Jaarlijkse rapportage aangaande AVG/ dataprivacy en monitoring daarvan in het afgelopen jaar en vooruitblik naar komend jaar.

De contactgegevens van de FG zijn:

Jan Schilt / P1P2
t.a.v. FG-Stichting Pensioenfonds Croda
Postbus 4122
5604 EC Eindhoven
e-mail: FG-pensioenfondsCroda@p1p2.nl

3.3 Inschakeling van verwerkers

Het fonds dient 'in control' te zijn voor zijn uitbestede werkzaamheden. Het fonds is eindverantwoordelijk voor de werkzaamheden die zij heeft uitbesteed. Het fonds houdt daarom toezicht op de verwerkingen die door de verwerker(s) worden uitgevoerd. Het fonds doet uitsluitend een beroep op een verwerker, die:

- afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen biedt, zodat de verwerking van persoonsgegevens aan de bepalingen van de AVG voldoet;
- Afdoende garanties biedt dat haar privacybeleid niet strijdig is met het privacybeleid van het fonds.

De afspraken met verwerkers worden vastgelegd in een schriftelijke verwerkersovereenkomst. De verwerkersovereenkomst legt ten minste de verplichtingen als bedoeld in artikel 28, lid 3 (onder a tot en met h) AVG op aan de verwerker.

3.4 Accountant, actuaris

In verband met controles ten behoeve van de certificering hebben de accountant en de actuaris van het fonds, als Verwerkingsverantwoordelijke, toegang tot de persoonsgegevens. Zij tekenen daartoe een geheimhoudingsverklaring.

4. Risico's

Om tot een solide en effectief privacybeleid te komen, is geïdentificeerd welke risico's zich op dit gebied kunnen voordoen. Voor zover nodig zijn passende maatregelen ter zake genomen. Deze zijn verwerkt in het risicomanagement van het pensioenfonds.

Risico's kunnen zich voordoen bij onvoldoende borging van het privacybeleid en kunnen gevolgen hebben voor de organisatie. Deze gevolgen kunnen worden opgesplitst in de volgende drie schadecategorieën.

Reputatieschade: Privacy risico's waardoor het imago van het fonds schade lijdt door het bekend worden van feiten of omstandigheden of door publieke beeldvorming, als gevolg waarvan het vertrouwen in de organisatie wordt geschaad.

Juridisch en regelgevingschade: Privacy risico's waardoor het fonds te maken krijgt met inspecties of juridische procedures, met als gevolg sancties of (andere) onvoorziene uitgaven. Dit kan aan de orde zijn als het vermoeden bestaat dat het beleid op het gebied van privacy van het fonds niet toereikend is.

Operationele schade: Privacy risico's waardoor het fonds tekort schiet op het vlak van privacy management. Ook kan administratieve overbelasting ontstaan, bij werkgevers, wanneer privacy problemen aanleiding geven tot misverstanden en daaraan gekoppelde gedragingen, individuele klachten, verzoeken of claims.

5 Privacy management

5.1. Beveiliging en geheimhouding

Het fonds zorgt er al bij het ontwerpen van producten en diensten voor dat persoonsgegevens goed worden beschermd (privacy by design). De gegevens worden goed beveiligd. Dat kan bijvoorbeeld door het verlenen van autorisaties aan daartoe aangewezen personen en het pseudonimiseren (dan wel anonimiseren) van persoonsgegevens. De standaardinstellingen zijn zodanig dat de privacy wordt gewaarborgd (privacy by default). Indien toestemming van een betrokkene is vereist dient deze toestemming altijd vrijelijk, specifiek, geïnformeerd en ondubbelzinnig te zijn.

Het fonds houdt de persoonsgegevens geheim voor onbevoegden en personen die niets met de verwerking van doen hebben. Het fonds deelt persoonsgegevens niet met derden, tenzij de wet of de rechter het fonds daartoe verplicht, of als het de verwerker betreft.

5.2. Ketenverantwoordelijkheid

Het fonds vergewist zich ervan dat de verwerker persoonsgegevens beschermt met passende organisatorische en/of technische beveiligingsmaatregelen die redelijke waarborgen bieden tegen risico's van verlies of ongeautoriseerde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens. Het fonds verlangt hiervoor van de verwerker een verwerkersovereenkomst en dat de verwerker met eventuele subverwerkers een verwerkersovereenkomst heeft gesloten.

5.3. Datalekken

Persoonsgegevens moeten beveiligd zijn. Er is sprake van een datalek als er sprake is van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Het fonds registreert alle datalekken. Het fonds meldt een datalek aan de Autoriteit Persoonsgegevens als het datalek persoonsgegevens van gevoelige aard betreft, zoals

- gegevens over de financiële of economische situatie: zoals salaris en pensioengegevens; gebruikersnamen en inlogcodegegevens die kunnen leiden tot persoonsfraude, zoals BSN, paspoort of identiteitskaart of rijbewijs;
- in het geval dat er een aanzienlijke kans is dat er ernstige nadelige gevolgen zijn voor de bescherming van persoonsgegevens.

Indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene, stelt het fonds ook betrokkene van het datalek op de hoogte. Het fonds vergewist zich ervan dat een verwerker datalekken registreert en doorgeeft via de FG aan de Autoriteit Persoonsgegevens en de betrokkene.

Klachten inzake een datalek kunnen aan de FG worden gericht.

5.4 Register van de verwerkingsactiviteiten

Het fonds houdt een register van de verwerkingsactiviteiten bij die onder zijn verantwoordelijkheid plaatsvinden. Het register bevat in ieder geval alle volgende gegevens:

1. de naam en de contactgegevens van het pensioenfonds;
2. de naam en contactgegevens van de Functionaris Gegevensbescherming;
3. de verwerkingsdoeleinden;
4. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
5. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
6. doorgiften van persoonsgegevens aan een derde land of een internationale organisatie;
7. de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
8. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het register is in elektronische vorm opgesteld. Desgevraagd stelt het fonds het register ter beschikking van de Autoriteit Persoonsgegevens.

5.5. Te verstrekken informatie

Het fonds verstrekt de betrokkene de wettelijk voorgeschreven informatie

- door middel van de privacyverklaring en cookieverklaring op de website;
- via de werkgever door middel van een informatietekst;
- door middel van de informatietekst bij de wettelijk voorgeschreven informatie.

Het fonds verstrekt de hiervoor genoemde informatie, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt.

5.6 Rechten van betrokkene

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkene genoemd, en bestaan uit de volgende rechten:

5.6.1 Recht op informatie

Betrokkenen hebben het recht om aan het fonds te vragen of zijn/haar persoonsgegevens worden verwerkt en welke dat zijn.

5.6.2 Recht van inzage

Betrokkene heeft het recht om van het fonds duidelijkheid te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;
- wanneer de persoonsgegevens niet bij het fonds worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van de profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen.

Het fonds verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan het fonds op basis van de administratieve kosten een redelijke vergoeding aanrekenen.

Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

5.6.3 Recht op rectificatie

De betrokkene heeft het recht om van het fonds onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervolledigen van onvolledig persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Het fonds stelt de betrokkene aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Het fonds verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

5.6.4 Recht op beperking van de verwerking

De betrokkene heeft het recht van het fonds de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die het fonds in staat stelt de juistheid van de persoonsgegevens te controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- het fonds heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van het fonds zwaarder wegen dan die van de betrokkene.

Wanneer de verwerking is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

De betrokkene die een beperking van de verwerking heeft verkregen, wordt door het fonds op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

Het fonds stelt de betrokkene aan wie persoonsgegevens zijn verstrekt, in kennis van elke beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Het fonds verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

5.6.5 Recht op gegevenswissing („recht op vergetelheid")

De betrokkene heeft het recht van het fonds zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en het fonds is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:

a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
b) de betrokkene maakt bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking;
c) de persoonsgegevens zijn onrechtmatig verwerkt;
d) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Europees of het Nederlands recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

Het fonds bewaart de persoonsgegevens zo lang als nodig is voor de uitvoering van de pensioenregeling of de wettelijke verplichtingen. De reden hiervoor is dat een vordering van pensioen niet verjaart tijdens het leven van een pensioengerechtigde. Om een eventuele juistheid van een pensioen, of om te kunnen aantonen dat een claim onterecht is, hoeft het fonds het recht op gegevenswissing niet te honoreren. De persoonsgegevens zijn gedurende de periode dat een vordering nog niet is verjaard nodig voor het doeleinde waarvoor ze zijn verzameld of verwerkt, zodat a niet aan de orde is. Bovendien is het voor het fonds een prevalerende dwingende gerechtvaardigde grond als bedoeld onder b voor de in stand houding van de gegevens is. Het fonds werkt daarom alleen mee aan het wissen van persoonsgegevens als dat moet op grond van c of d.

Wanneer het fonds de persoonsgegevens openbaar heeft gemaakt en verplicht is op verzoek de persoonsgegevens te wissen, neemt het fonds, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om uitvoerders die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene het fonds heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Het voorgaande is niet van toepassing voor zover verwerking nodig is:

a) voor het nakomen van een in een het Europees recht of het Nederlands recht neergelegde wettelijke verwerkingsverplichting die op het fonds rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan het fonds is verleend;
b) om redenen van algemeen belang op het gebied van volksgezondheid;
c) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden voor zover het recht op gegevenswissing de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
d) voor het fonds, uitoefening of onderbouwing van een rechtsvordering.

Het fonds stelt de betrokkene aan wie persoonsgegevens zijn verstrekt, in kennis van elke wissing van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Het fonds verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

5.6.6 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt, indien:

- de verwerking berust op toestemming, of op een overeenkomst en
- de verwerking via geautomatiseerde procedés wordt verricht.

Het recht op dataportabiliteit is geen algemeen recht in de gevallen dat de verwerking niet is gebaseerd op instemming of een overeenkomst. Voor werknemers gaat het om gegevens die op grond van de arbeidsovereenkomst verschaft worden en niet op basis van wettelijke voorschriften verschaft moeten worden.

Het fonds handelt ten opzichte van werknemers niet in concurrentie met andere pensioenuitvoerders en de betrokkene heeft geen vrije keuze tussen pensioenfondsen. Het doel van dataportabiliteit is daarom bij een pensioenfonds niet aan de orde.

Voor de verwerking van de persoonsgegevens is geen instemming van de betrokkene nodig. Daarom werkt het fonds niet mee aan geautomatiseerde gegevensverschaffing en doorlevering van persoonsgegevens.

5.6.7 Recht op bezwaar

Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. Gezien de gerechtvaardigde gronden voor de verwerking kan het fonds hier niet aan voldoen.

5.6.8 Recht niet onderworpen te worden aan geautomatiseerde besluiten

Het fonds maakt geen gebruik van profilering.

5.7 Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden bij het fonds.

Het fonds heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal het fonds laten weten wat er met het verzoek gaat gebeuren. Als het verzoek complex is of als er een aantal verzoeken is, kan de periode voor het beantwoorden met nog eens twee maanden worden verlengd. De reden van de vertraging moet aan betrokkene worden meegedeeld. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij het fonds, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

Aan de hand van een verzoek kan het fonds aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. Hiervoor worden geen kosten in rekening gebracht, tenzij er sprake is van een buitensporig verzoek.

5.8 Klachten

Eventuele conflicten of meningsverschillen in verband met de eisen op grond van dit privacybeleid of andere eisen die verband houden met gegevensbescherming kunnen ter beslechting worden voorgelegd aan de Klachten en geschillencommissie van het Fonds conform het terzake geldende reglement. In geval van een klacht inzake een datalek betreft geldt hetgeen in 5.3 is beschreven.

5.9 Verplichting jegens Autoriteit Persoonsgegevens

Het fonds reageert tijdig en adequaat op verzoeken van de Autoriteit Persoonsgegevens of een andere bevoegde autoriteit. Vragen kunnen betrekking hebben op de meldingen van de gegevensverwerking aan de Autoriteit Persoonsgegevens of meer in het algemeen op naleving van de toepasselijke privacy wet- en regelgeving. Het bestuur en/of medewerkers van verwerkers van het fonds die een dergelijk verzoek van de Autoriteit Persoonsgegevens ontvangen, nemen direct contact op met de FG. De FG zal te allen tijde betrokken worden in de communicatie met de Autoriteit Persoonsgegevens of een andere bevoegde autoriteit.

6. Evaluatie en monitoring

6.1. Evaluatie

Het fonds evalueert en past dit beleid zo nodig aan, indien daarvoor aanleiding is op basis van andere gebruiken, wijzigende wet- en regelgeving en aanwijzing van de Autoriteit Persoonsgegevens. Het pensioenfonds evalueert dit beleid periodiek.

6.2. Monitoring

Het bestuur controleert de naleving van het beleid op basis van de rapportages van de verwerkers en van de contactpersoon gegevensbescherming. De monitoring van het beleid is belegd bij de FG, en de contactpersoon gegevensbescherming van het fonds

7. Toepasselijkheid en inwerkingtreding

Dit privacybeleid is in december 2018 vastgesteld door het bestuur van het fonds.

Dit beleid is met onmiddellijke ingang van toepassing op alle activiteiten die gepaard gaan met de verwerking van persoonsgegevens door of namens het fonds en door personen die onder de leiding of het beheer van het fonds werken.

Het pensioenfonds erkent dat het mogelijk is dat de Nederlandse wetgeving zwaardere, strengere en/of afwijkende normen voor de bescherming van persoonsgegevens oplegt. De Nederlandse wetgeving is te allen tijde van toepassing en prevaleert boven dit beleid, indien en voor zover zij de normen van dit beleid overtreft, strengere eisen oplegt en/of meer bescherming biedt. Wanneer dit beleid meer bescherming biedt dan de Nederlandse wetgeving of voorziet in extra voorzorgsmaatregelen, rechten of rechtsmiddelen voor betrokkenen, is dit beleid van toepassing.

Bijlage: Raamwerk procedure aanvraag betrokkene om rechten uit te oefenen

INTRODUCTIE
Betrokkenen hebben een aantal rechten met betrekking tot hun persoonlijke gegevens. Deze checklist biedt een raamwerk dat kan worden gebruikt om geschikte interne processen vast te stellen met als doel te reageren op dit soort verzoeken van betrokkenen.

Wanneer het fonds een verzoek van betrokkene krijgt, moet er een procedure zijn die iemand of meer dan één persoon de verantwoordelijkheid geeft om stappen te ondernemen. Er zijn vaak drie personeelsniveaus bij de behandeling van een verzoek betrokken:

1. **de leidinggevende persoon:** neemt de algehele verantwoordelijkheid om ervoor te zorgen dat een correct antwoord wordt gestuurd en die, indien nodig al dan niet via de FG, contact onderhoudt met de relevante toezichthoudende autoriteit;
2. **operationeel manager**: verantwoordelijk voor het instrueren van personeel om te zoeken naar relevante gegevens; de toegang tot individuele mailboxen goedkeuren; beslissen over moeilijke kwesties zoals gevoelige redacties of, in marginale gevallen of gegevens persoonlijke gegevens zijn; waar gegevens betrekking hebben op andere personen, beslissen of toestemming wordt gevraagd of dat het redelijk is om zonder toestemming te onthullen; en het finaliseren en goedkeuren van de informatie in het antwoord.
3. **operationele en administratieve ondersteuning**: met betrekking tot het lokaliseren van gegevens; het doorzoeken van de gegevens (en het registreren van uitgevoerde zoekopdrachten); en het identificeren van gegevens met betrekking tot andere individuen en, indien van toepassing het verkrijgen van toestemming.
   Input van IT afdeling kan ook gewenst zijn, vooral als toegang tot individuele mailboxen vereist is.

Het personeel dat aan het verzoek werkt moet voldoende opgeleid zijn om zijn of haar taken uit te voeren.

REAGEREN OP HET VERZOEK

1. Controleer of een verzoek gerechtvaardigd is, wordt er terecht een beroep gedaan op de rechten van betrokkene uit de AVG of heeft het verzoek een andere lading (voorbeeld klacht of geschil).

2. Bepaal wie wat gaat doen.

3. Maak een eerste beoordeling:
   - Registreer de datum waarop het verzoek is ontvangen, bereken de uiterste datum voor reactie (reactietermijn is 30 dagen);
   - Controleer de identiteit van de betrokkene die het onderwerp is van het verzoek. In geval van twijfel kan aanvullende informatie worden opgevraagd om de identiteit van betrokkene te (laten) bevestigen;
   - Beslis of de reikwijdte van het verzoek van betrokkene moet worden verduidelijkt en wat hij of zij wil;
   - Overweeg of het verzoek kennelijk ongegrond of buitensporig is (bijvoorbeeld vanwege het herhalende karakter ervan) en zo ja, na te gaan of er een redelijke vergoeding in rekening kan worden gebracht;
   - Maak, indien praktisch uitvoerbaar, een ruwe schatting van het aantal te controleren documenten.

4. Bepaal of de reactietermijn naar betrokken moet worden verlengd (bijvoorbeeld bij complexe verzoeken) en zo ja, met welke termijn. Bepaal de reden van vertraging en stel de betrokkene hiervan op de hoogte binnen 30 dagen (verlenging maximaal 2 maanden).

5. Zoek in databases, systemen, applicaties en andere plaatsen waar persoonlijke gegevens worden bewaard:
   - identificeer pool van gegevens die persoonlijke gegevens over de betrokkene zijn;
   - proberen de gegevens in de pool te beperken met behulp van geschikte criteria;
   - herzien van de gegevens om te zien of deze gegevens bevatten met betrekking tot andere personen;

- beslissen of toestemming van andere personen moet worden gevraagd, of zonder toestemming bekend mag worden gemaakt of mag worden geweigerd om bekend te maken;
- finaliseer de kopiegegevens die openbaar moeten worden gemaakt.

6. Bereid antwoord naar betrokkene voor met kopieën van documenten en informatie over:
    - doeleinden van verwerking;
    - categorieën van persoonlijke gegevens;
    - ontvangers of categorieën ontvangers;
    - informatie over de bron van persoonsgegevens;
    - bewaartermijnen;
    - bestaan van rechten van betrokkenen;
    - bestaan van geautomatiseerde besluitvorming inclusief profilering;
    - waarborgen bij overdrachten buiten de EER; en
    - recht om te klagen bij een toezichthoudende autoriteit.

    Bij rectificatie moet in het antwoord naar betrokkene melding worden gemaakt van elke rectificatie of beperking van de verwerking.

    Bij gegevenswissing moet in het antwoord naar betrokkene melding worden gemaakt van elke wissing van persoonsgegevens.

    Bij beperking moet in het antwoord naar betrokkene melding worden gemaakt van elke beperking van de verwerking.