Verwerkingsverantwoording en register van verwerkingsactiviteiten
180904-NOT-GRP-VerantwoordingsplichtAVG
Stichtingen PK, U Centraal, JoU en Specifieke Jeugdprojecten

Ter inleiding

De Algemene Verordening Gegevensbescherming (AVG) schrijft de organisatie voor om middels een document aan te tonen dat wordt voldaan aan de wetgeving bij de verwerkingen van persoonsgegevens.

Verantwoordingsplicht	
Verwerkingsverantwoording	Verwerkingsregister

Met dit document, de verwerkingsverantwoording, voldoet de organisatie aan de zogenaamde verantwoordingsplicht.
Een tweede onderdeel van de verantwoordingsplicht is het verantwoordingsregister. In dit register wordt per organisatie en vervolgens per project/afdeling precies aangegeven welke gegevens worden verwerkt, met welk doel dit gebeurt, hoe de gegevens zijn verkregen, welke gegevens hiervan bijzondere persoonsgegevens zijn, wat de noodzaak is deze bijzondere persoonsgegevens te verwerken, hoe lang de gegevens worden bewaard en met wie deze worden gedeeld.

De verwekingsverantwoording en/of het verwerkingsregister wordt bij organisatorische wijzigingen met grote gevolgen voor de gegevensverwerking tussentijds gewijzigd. Daarbij worden beide documenten jaarlijks (4^{e} kwartaal) geactualiseerd door de Functionaris Gegevensbescherming in nauwe samenwerking met het Hoofd Compliance.

Zowel de Verwerkingsverantwoording als het verwerkingsregister als relevante documenten waarnaar in de verwerkingsverantwoording wordt verwezen zijn digitaal beschikbaar voor alle betaalde medewerkers van de organisatie op een speciaal daarvoor ingerichte plek.
De verwerkingsverantwoording is online beschikbaar zodat een ieder die dit wenst het kan raadplegen.

De Verwerkingsverantwoording

1. Algemene informatie

In deze notitie spreken we over het samenwerkingsverband van de stichtingen U Centraal, PK, Specifieke Jeugdprojecten, JoU en Ravelijn als “de groep” en over de afzonderlijke onderdelen als een “lid van de groep” om zo te voorkomen dat er meerdere benamingen gebruikt gaan worden voor hetzelfde. De leden van de groep, te weten vijf stichtingen, vormen samen een personele unie. Zij delen een Raad van bestuur en Raad van Toezicht. De stichtingen U Centraal, Specifieke Jeugdprojecten en JoU voeren werkzaamheden in het kader van de WMO en Jeugdwet uit. Stichting PK biedt hen hierbij de benodigde ondersteuning. Stichting Ravelijn is een stichting zonder personeel en uitvoerende activiteiten.

De leden van de groep hebben ten doel:
“Het ondersteunen en hulp bieden aan mensen en zo bijdragen aan hun kwaliteit van leven, op een wijze die respectvol, passend en daardoor effectief is voor iedere specifieke situatie;
door het in stand houden van een organisatie ter realisering van dit doel;
en voorts al hetgeen daarmee rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de meest ruime zin van het woord.”

De leden van de groep hebben geen winstoogmerk, haar financiële middelen en alle andere eventuele vermogensbestanddelen dienen ten goede te komen aan het sociaal domein.

In onze groep van organisaties wordt samengewerkt op basis van een gemeenschappelijke visie en een overeenkomstige bedrijfsmatige opzet. Deze inhoud van samenwerking wordt samen vormgegeven en wordt zo door ieder lid van de groep gedragen.
Deze samenwerking wordt dagelijks in de praktijk gebracht maar laat onverlet dat elk lid van de groep ook zijn eigenheid heeft:

- Het Bedrijfsbureau PK legt zich toe op het uitvoeren van bedrijfsmatige processen die in alle andere organisaties nodig zijn. De kwaliteit van die uitvoering is essentieel voor het belang dat elke organisatie hecht aan de samenwerking.
- JoU geeft uitvoering aan het jongerenwerk in de stad Utrecht en heeft dus een hele specifieke doelgroep die daarmee ook bepalend is voor de eigenheid die JoU nodig heeft om hen te bereiken en jongerenwerk te doen.
- Pretty Woman, Back UP, Fiom Utrecht, Home-Start, OWR en PPI zijn specifieke jeugd projecten (SJP) die elk een hele specifieke doelgroep hebben en daarbij behorende problematiek trachten te voorkomen of verhelpen.
- Ravelijn werkt regionaal en richt zich specifiek op vrijwillige inzet in het sociaal domein en op mantelzorgondersteuning. Eind 2016 zijn haar activiteiten in Amersfoort gestopt maar mogelijk zal een doorstart in de toekomst worden vormgegeven.
- U Centraal werkt in de stad en regio Utrecht aan:
    - Informatie & Advies, Onafhankelijke Cliëntondersteuning en Schulddienstverlening.
    - Activiteiten van Informele Zorg en Mantelzorgondersteuning.
    - Wonen: Buurtbemiddeling, Woonoverlast en Ernstig Overlastgevende Gezinnen.
    - Maaltijden Service

De groep wordt geleid door een directieraad met daarin directie/hoofden, bestuurssecretaris, hoofd compliance, controller en Raad van Bestuur.
De groep noch de leden van de groep deelt persoonsgegevens met internationale organisaties.

2. Doel van de verwerking

Het is voor het realiseren van het doel van de groep noodzakelijk dat de organisatie persoonsgegevens van cliënten (of: jongeren, deelnemers, klanten), vrijwilligers, beroepskrachten en stagiairs verwerkt.
De organisatie wil en is wettelijk verplicht om zorgvuldig om te gaan met deze persoonsgegevens. De groep heeft dan ook een privacyreglement.

De groep legt de persoonsgegevens van de cliënt vast die noodzakelijk zijn voor het zorgvuldig uitvoeren van de dienstverlening aan de cliënt. Dienstverlening die bestaat uit het ondersteunen en hulp bieden aan mensen en zo bijdragen aan hun kwaliteit van leven, op een wijze die respectvol, passend en daardoor effectief is voor iedere specifieke situatie. De groep realiseert dit doel door de inzet van beroepskrachten, stagiairs en vrijwilligers.

De groep legt de persoonsgegevens van de vrijwilliger vast die noodzakelijk zijn voor een zorgvuldige uitvoeren van het vrijwilligersbeleid. De persoonsgegevens van een vrijwilliger die zijn opgenomen in het bestand worden verwijderd uiterlijk twee jaar nadat deze niet meer werkzaam is voor de organisatie, met uitzondering van de gegevens die langer moeten worden bewaard als gevolg van fiscale regelgeving.

De groep legt de persoonsgegevens van de beroepskracht vast die noodzakelijk zijn voor het zorgvuldig uitvoeren van het personeelsbeleid. De persoonsgegevens van een beroepskracht die zijn opgenomen in het bestand worden verwijderd uiterlijk zeven jaar nadat deze niet meer werkzaam is voor de organisatie.

De groep de persoonsgegevens van de stagiair vast die noodzakelijk zijn voor een zorgvuldige begeleiding in het kader van de opleiding. De persoonsgegevens van een stagiair die zijn opgenomen in het bestand worden verwijderd uiterlijk zeven jaar nadat deze niet meer werkzaam is voor de organisatie.

3. Grondslag verwerking persoonsgegevens

Voor het verwerken van persoonsgegevens van medewerkers, vrijwilligers en stagiaires is de grondslag ‘uitvoering van de overeenkomst’ de grondslag: een medewerker, vrijwilliger of stagiair wenst te komen werken bij één van de leden van de groep. Verwerking van persoonsgegevens komt in dit geval logischerwijs voort uit de overeenkomst die wordt aangegaan.

Voor het verwerken van persoonsgegevens van cliënten is in bijna alle gevallen ‘uitvoering van de overeenkomst’ de grondslag: een cliënt meldt zich bij één van de leden van de groep aan of laat zich verwijzen. Verwerking van persoonsgegevens komt in dit geval logischerwijs voort uit deze aanmelding of verwijzing. Hierop gelden enkele belangrijke uitzonderingen:

3.1 Toestemming van ouders

In geval van hulp of ondersteuning aan minderjarige kinderen is toestemming van ouders grondslag voor de verwerking. Toestemming van beide ouders met gezag is grondslag in geval van een hulp- of ondersteuningsaanbod. In geval van deelname aan een activiteit zonder dat hierbij wordt gewerkt van individuele doelen of leerpunten volstaat de toestemming van één ouder met gezag om deze aanpak zo laagdrempelig mogelijk te houden.

3.2 Convenantafspraken

Verwerken van persoonsgegevens met convenantafspraken als basis waarin een andere grondslag is vastgelegd:

- PGA groepsaanpak met bijbehorende privacyreglement, JoU
- Verwijsindex
- Overeenkomst woonproblematiek, U Centraal

4. Informatieplicht

De organisatie informeert de cliënt bij het eerste contact, of anders zo spoedig mogelijk, over de verwerking van persoonsgegevens. De beroepskracht of vrijwilliger maakt hierbij zelf de afweging of dit mondeling (met aantekening in cliëntdossier of bestand) dan wel schriftelijk gebeurt. De cliënt wordt geïnformeerd over welke gegevens worden vastgelegd, met welk doel dit gebeurt, hoe lang de gegevens worden bewaard, welke rechten de betrokkene kan uitoefenen ten aanzien van de verwerking van zijn gegevens en tot wie hij zich voor de uitoefening van deze rechten moet wenden. Het feit dat de organisatie een Functionaris Gegevensbescherming heeft en hoe deze te bereiken is

wordt hierbij ook bekend gemaakt.
Op de diverse websites van de groep is alle informatie terug te lezen: de verwerkingsverantwoording, het privacybeleid en een algemeen verhaal, in heldere en begrijpelijke taal, over de omgang van de groep met persoonsgegevens.

Bij de aanstelling van een nieuwe medewerker of stagiair zorgt de afdeling administratie ervoor dat aan de informatieplicht wordt voldaan: de nieuwe collega wordt geïnformeerd over welke gegevens met wie en om welke reden worden gedeeld, welke bewaartermijnen worden gehanteerd, welke rechten de betrokkene kan uitoefenen ten aanzien van de verwerking van zijn gegevens en tot wie hij zich voor de uitoefening van deze rechten moet wenden.

Vrijwilligers worden in de vrijwilligersovereenkomst gewezen op het feit dat gegevens worden vastgelegd en welke rechten er ten aanzien van deze gegevens van kracht zijn.

5. Verstrekking van persoonsgegevens

Voor het verstrekken van gegevens van cliënten is gerichte en ondubbelzinnige toestemming de grondslag. Hiervan wordt een aantekening gemaakt in het cliëntdossier of een formulier ingevuld dat aan het cliëntdossier wordt toegevoegd.

Het overleggen met directe collega's over het hulpaanbod aan de cliënt, bijvoorbeeld in een casuïstiekbespreking, gebeurt binnen een team of afdeling dat gezamenlijk aan hetzelfde primair proces werkt en alleen daar waar het bijdraagt aan de hulp of ondersteuning aan de cliënt. Hiervoor is toestemming van cliënt niet nodig. Buiten afdelingen of teams om is de toestemming wel de grondslag om te mogen overleggen, ook al delen medewerkers een werkgever.

Voor verstrekking van persoonsgegevens van kinderen tot 16 jaar geldt de toestemming van alle ouders met gezag en dat van het kind (mits ouder dan 12 jaar) als grondslag.
Vrijwillige medewerkers verstrekken alleen als daarvoor ondubbelzinnige toestemming van de cliënt is.

Verstrekking vindt op casus-niveau plaats en gebeurt aan samenwerkingspartner of mensen uit het netwerk van de desbetreffende cliënt. In de regel verstrekt de groep nooit massaal persoonsgegevens van cliënten. Uitzondering hierop is de wettelijk verplichte verstrekking van persoonsgegevens van cliënten die gebruik maakten van Jeugdzorg aan het CBS. De aanlevering gebeurt digitaal en wordt door het CBS versleuteld voor verdere verwerking.

Er zijn enkele uitzonderingen op verstrekken met als grondslag toestemming:

- Vitaal belang als grondslag: in een enkel geval geldt het vitaal belang van de cliënt als grondslag om te verstrekken. Dit komt voor daar waar gewerkt wordt met cliënten met ernstige meervoudige problematiek, te denken valt aan Back Up en Woonoverlast. In die uitzonderlijke gevallen gaat de beroepskracht over tot verstrekken van persoonsgegevens omdat hulp aan een cliënt wiens vitaal belang in het geding is te organiseren of bieden. De medewerker maakt van de genomen beslissing en afweging een aantekening in het cliëntdossier en informeert de cliënt zo snel mogelijk van dit feit.
- Verstrekken met convenantafspraken als basis waarin een andere grondslag is vastgelegd:
- PGA groepsaanpak met bijbehorende privacyreglement, JoU
- Verwijsindex, JoU/ U Centraal/ SJP
- Overeenkomst woonproblematiek, U Centraal

- Stichting PK verstrekt gegevens van medewerkers om hiermee aan (fiscale) regelgeving te voldoen. Medewerkers worden hiervan bij aanstelling éénmalig op de hoogte gebracht. Wanneer Stichting PK sporadisch gegevens van vrijwilligers (in geval van onkostenvergoeding hoger dan wettelijke grens) of zelfstandig werkende (in geval van ínkomsten uit overige werkzaamheden) aan de belastingdienst moet verstrekken a.g.v een wettelijk plicht dan wordt de betrokkene hiervan achteraf per brief op de hoogte gesteld.

6. Inhuur van verwerkers

Voor de inhuur van gegevensverwerkers geldt het regelement inhuur van externen (onderdeel van het handboek kwaliteit). De gegevenensverwerker en de verwerkingsverantwoordelijke maken werkafspraken die vallen binnen de kaders van de AVG. Dit is voor de groep een voorwaarde om met een verwerker in zee te gaan. De afspraken worden vastgelegd in een verwerkersovereenkomst.

De groep heeft met de volgende verwerkers een verwerkersovereenkomst:

Verwerker	Doel/werkzaamheden	Overeenkomst met
Kompas Veiligheidsgroep	Verwerking van gegevens personeel t.b.v. BHV cursusaanbod/certificaten.	Stichting PK, voor de hele groep
Involvit	Websitebouwer en beheerder	Stichting PK, voor de hele groep
CCV	Client- en vrijwilligersregistratie t.b.v Buurtbemiddeling	U Centraal (Buurtbemiddeling)
MicPoint	Ritregistratie van JoU voertuigen	Stichting PK
VWO Zorg van de Zaak	ARBOdienst, registratie personeelsgegevens	Stichting PK, voor de hele groep
Winvision	Systeembeheerder extern bureaublad	Stichting PK, voor de hele groep
Royal Foods	Verwerking klantgegevens maaltijdenservice	U Centraal (maaltijdenservice)
Efficiency Online	Client- en vrijwilligersregistratie t.b.v Home Start	SJP (Home Start)
Stichting nationaal ouderenfonds	Client- en vrijwilligersregistratie t.b.v DomStadPlusBus	U Centraal (DomstadPlusBus)

7. Data bescherming

Stichting PK is binnen de groep verantwoordelijk voor het beschikbaar stellen van middelen om persoonsgegevens van cliënten en medewerkers passend te beveiligen. Dit gebeurt door te zorgen voor digitale beveiliging, beveiliging van persoonsgegevens op papier en het instrueren van medewerkers over het gebruik hiervan.

Het hoofd compliance, lid van de directieraad, is verantwoordelijk voor het voldoen van de AVG. Het hoofd werkt daartoe nauw samen met de Functionaris Gegevensbescherming (FG) en, daar waar het gaat om de digitale en fysieke bescherming van persoonsgegevens, met de afdeling ICT (Stichting PK).

7.1 Fysieke beveiliging

In de organisatie wordt in principe papierloos gewerkt. Alleen daar waar het gebruik van papier uitlegbaar is wordt hiervan gebruik gemaakt.
Papieren met daarop persoonsgegevens worden bewaard in kasten met sloten.

7.2 Digitale beveiliging
De groep beveiligd digitaal opgeslagen persoonsgegevens passend.

7.2.1 Toegang tot het extern bureaublad
De digitale werkomgeving is op desktops en laptops bereikbaar na dubbele authenticatie: met de combinatie van een gebruikersnaam en wachtwoord en met een token (Microsoft EMS). De medewerkers worden iedere drie maanden verzocht het wachtwoord te vernieuwen.
Vrijwilligers die persoonsgegevens van clienten verstrekken, bijvoorbeeld door het geven van een terugkoppeling aan een medewerker van de groep of een samenwerkingspartner, doen dit binnen de beveiligd omgeving van het extern bureaublad in een office 365 omgeving die door de organisatie aan hen ter beschikking wordt gesteld.

7.2.2 Toegang tot outlook op de telefoon
Alleen op telefoons die zijn beveiligd met een pincode, patroon of vingerafdruk kan outlook worden geopend en gelezen. Installatie van outlook op de telefoon gebeurt met dubbele authenticatie van gebruikersnaam met wachtwoord en een token.

7.2.3 AFAS Profit
Het programma Profit wordt gebruikt voor de cliënt-, salaris-, project-, ordermanagement-, personeels- en financiële administratie. Door middel van autorisatie zijn bepaalde gegevens alleen toegankelijk voor geautoriseerde medewerkers. Autorisatie verloopt geautomatiseerd op basis van formatie: teams hebben veelal toegang tot dezelfde cliëntgegevens. Bij vrijwilligers wordt dit door enkele medewerkers geautoriseerd in Profit. De (financiële) administratie wordt handmatig geautoriseerd. Deze laatste handmatige autorisatie wordt door het afdelingshoofd in de gaten gehouden en gecontroleerd door de extern accountant. Profit is alleen toegankelijk voor gebruikers met ‘active directory account’ en ‘two factor autorisatie’ d.m.v. een token.

7.2.4 Toegang tot bestanden op (lokale) schijven
Een geautomatiseerde autorisatie op basis van formatie biedt al dan geen toegang tot bepaalde lokale schijven. Zo hebben alleen de medewerkers die deel uitmaken van een bepaald team of een bepaalde afdeling toegang tot lokale schijven die zij voor hun werkzaamheden nodig hebben. Vrijwilligers worden d.m.v. gegevens vanuit Profit geautoriseerd door enkele daarvoor aangewezen medewerkers.
Om ongegronde toegang van medewerkers tot informatie op de lokale schijf te voorkomen voert de afdeling ICT ieder kwartaal een handmatige check uit. Leidinggevenden ontvangen een overzicht met waarin autorisaties die niet automatisch op basis van formatie zijn gedaan. Zij beslissen of de autorisatie ingetrokken moet worden of niet.

7.2.5 Voorkomen van een datalek
De volgende maatregelen worden genomen om de kans op een datalek te verkleinen:

- De organisatie hanteert een ICT protocol waaraan medewerkers zich hebben te houden. De regels ten aanzien van de omgang met hard- en software worden hierin beschreven. Het ICT protocol is onderdeel van het Handboek Kwaliteit.
- Medewerkers kunnen alleen beveiligd printen binnen het extern bureaublad en in de vaste panden van de organisatie. We voorkomen hiermee rondslingerende en achtergebleven papierwerk bij de printer.
- E-mails bij versturen van persoonsgegevens naar externen wordt versleuteld (TLS + EMS als alternatief).
- Hardware controle: bij inleveren en steekproefsgewijs wordt hardware door de afdeling ICT gecontroleerd op de (foutieve) opslag van persoonsgegevens.

- Toegangsbeveiliging: onderhoud van firewalls/vpn en Wi-Fi AP's vaste panden. De netwerken van de panden zijn beveiligd met hardware firewalls, verbindingen naar het datacenter verlopen via een beveiligde verbinding (VPN) en de Wi-Fi wordt via controleerbare Access points verzorgt en onderhouden.

7.2.6 DPIA

Onder de AVG kan de organisatie verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen, om vervolgens maatregelen te kunnen nemen en de risico's te verkleinen. De DPIA is niet verplicht voor de groep maar zal in 2018 en ieder daarop volgend jaar wel jaarlijks worden uitgevoerd door de afdeling ICT i.s.m. het hoofd bedrijfsbureau, Functionaris Gegevensbescherming (FG) en hoofd compliance.

7.2.7 Dataportabiliteit

Het systeem waarbinnen de groep zowel de gegevens van cliënten als die van vrijwilligers en medewerkers vastlegt biedt de mogelijkheid om persoonsgegevens digitaal beschikbaar te stellen aan de cliënt of, indien gewenst, digitaal te doen toekomen aan een andere partij. Zo kunnen gegevens worden hergebruikt. De manier die hiervoor wordt gebruikt hangt af van de wensen van de betrokken cliënt en de digitale mogelijkheden van de ontvanger.

8. Datalek

De organisatie doet de uiterste best om een datalek te voorkomen: door het geven van voorlichting aan medewerkers en door het beschikbaar stellen van digitale hulpmiddelen om de kans op een lek te verkleinen (7.2.5). Ondanks dat kan een datalek voorkomen. Medewerkers zijn geïnstrueerd dit zo snel als mogelijk digitaal te melden.

Een datalek melding gebeurt digitaal via het intranet. De melder vult de gegevens in die ook voor een evt. melding bij de Autoriteit Persoonsgegevens nodig zijn in. Na de digitale melding krijgt de Functionaris Gegevensbescherming en het hoofd compliance een melding. De FG beoordeelt de melding, neemt indien nodig contact op met de melder en andere betrokkenen en bepaalt en coördineert de vervolgstappen. De Functionaris Gegevensbescherming legt de genomen stappen en afwegingen vast als onderdeel van de digitale melding en verzorgd indien nodig een melding bij de Autoriteit Persoonsgegevens.
Alle datalekmelding zijn digitaal te raadplegen door de Functionaris Gegevensbescherming en het hoofd compliance en indien nodig in één overzicht weer te geven.

Herhaalde aandacht genereren voor (het voorkomen van) een datalek en de noodzaak dit te melden behoort tot het takenpakket van de Functionaris Gegevensbescherming.

9. Register van verwerkingsactiviteiten

In het register van verwerkingsactiviteiten wordt per organisatie en vervolgens per project/afdeling precies aangegeven welke gegevens worden verwerkt, met welk doel dit gebeurt, hoe de gegevens zijn verkregen, welke gegevens hiervan bijzondere persoonsgegevens zijn, wat de noodzaak is deze bijzondere persoonsgegevens te verwerken, hoe lang de gegevens worden bewaard en met wie deze worden gedeeld.

Het verwerkingsregister wordt bij organisatorische wijzigingen met grote gevolgen voor de gegevensverwerking tussentijds gewijzigd. Daarbij worden beide documenten jaarlijks (4^{e} kwartaal)

geactualiseerd door de Functionaris Gegevensbescherming in nauwe samenwerking met het hoofd compliance.

Het is digitaal beschikbaar voor alle betaalde medewerkers van de organisatie en kan indien nodig worden overlegd aan de Autoriteit Persoonsgegevens. Het gaat om de volgende bestanden:

- 180426-OVZ-SJP-DocumentatieplichtAVG
- 180524-OVZ-UCe-DocumentatieplichtAVG
- 180525-OVZ-PK-DocumenatietieplichtAVG
- 180524-OVZ-JoU-DocumentatieplichtAVG

Tot de groep behoort ook Stichting Ravelijn. Ravelijn voert geen werkzaamheden meer uit maar heeft wel een archief met cliënt- en personeelsdossiers. In 2018 moeten de vastgelegde gegevens, bewaartermijnen en opslagplaatsen verder worden onderzocht en net als voor de andere leden van de groep in een verwerkingsregister opgesomd.

10. Functionaris gegevensbescherming

De groep heeft per 1 juni 2018 een Functionaris voor de gegevensbescherming aangesteld. Haar taken zijn beschreven in een functieomschrijving. De Functionaris Gegevensbescherming combineert diens taken met andere werkzaamheden binnen de organisatie en is daarmee vier dagen per week bereikbaar voor vragen van medewerkers, samenwerkingspartners en/of anderen.

De Functionaris Gegevensbescherming is bereikbaar per mail: functionaris.gegevensbescherming@stichting-pk.nl en per telefoon: 0651749732.

De Functionaris Gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens onder nummer FG006342.